UDC 621.391
DOI: 10.15587/1729-4061.2016.75250

DEVELOPMENT OF MCELIECE MODIFIED ASYMMETRIC CRYPTO-CODE SYSTEM ON ELLIPTIC TRUNCATED CODES

S. Yevseiev
PhD, Associate Professor, Senior Researcher*
E-mail: serhii.yevseiev@m.hneu.edu.ua

K. Rzayev
PhD, Associate Professor**
E-mail: xazail49@mail.ru

O. Korol
PhD, Associate Professor*
E-mail: olha.korol@m.hneu.edu.ua

Z. Imanova
Assistant**
E-mail: zarife1955@mail.ru

*Information Systems Department
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
**Department of Computer Technology and Programming
Azerbaijan State University of Oil and Industry
Azadlyg ave., 20, Baku, Azerbaijan, AZ1010

Розглядаються загальна конструкція теоретико-кодових схем (ТКС), несиметрична крипто-кодова система (НККС) на основі ТКС Мак-Еліса на укорочених (модифікованих) еліптичних кодах. Пропонується математична модель НККС Мак-Еліса, алгоритми формування та розшифрування/розкодування криптограми/кодограми, аналізуються витрати на програмну реалізацію крипто-кодових засобів захисту інформації на основі ТКС Мак-Еліса

Ключові слова: несиметрична крипто-кодова система, теоретико-кодова схема, модифіковані перешкодостійкі коди

Рассматриваются общая конструкция теоретико-кодовых схем (ТКС), несимметричная крипто-кодовая система (НККС) на основе ТКС Мак-Элиса на укороченных (модифицированных) эллиптических кодах. Предлагается математическая модель НККС Мак-Элиса, алгоритмы формирования и расшифрования/раскодирования криптограммы/кодограммы, анализируются затраты на программную реализацию крипто-кодовых средств защиты информации на основе ТКС Мак-Элиса

Ключевые слова: несимметричная крипто-кодовая система, теоретико-кодовая схема, модифицированные помехоустойчивые коды

1. Introduction

Development of telecommunication systems in all areas of their use puts forward stricter requirements to the reliability and security of the entire data processing cycle. To ensure these criteria in telecommunication systems, software/firmware implementation means of error-correcting coding techniques (to ensure reliability) and cryptographic information transformation methods (providing security: confidentiality, integrity and availability), as well as data transfer protocols at different levels of the ISO/OSI model are used. A promising direction in the development of communications technologies and systems are integrated mechanisms that provide the required reliability and safety performance in a single software/hardware and software implementation. For this purpose, the authors suggest the use of the modified asymmetric crypto-code system based on the McEliece theoretical-code scheme (TCS) on elliptic shortened codes. This approach provides the required level of reliability of data transfer through the use of error-correcting coding techniques, and the use of the asymmetric cryptosystem provides the required level of cryptographic performance.

2. Literature review and problem statement

The development of communication technologies is closely related to the quality of services provided to end users of the system and determined by the indicators proposed in the standards and recommendations of the International Communication Union. Among the main service quality indicators discussed in Recommendations ITU E.800, special importance is given to the coefficient of system availability, which provides the required level of reliability and security of the entire data processing and storage cycle [1, 2]. The analysis in the paper [3] showed that the rapidly growing number of users and information consumers, expanding the range of telecommunication services, increased volumes of processed data lead to a tightening of probability-time requirements for the major components of telecommunication systems and networks at all stages of the information data exchange. Thus, according to [4], the relevance of creating telecommunication systems and networks with protected data transmission channels has increased dramatically in recent years. The requirements for data security indicators in telecommunication systems and networks, especially in special-purpose networks in which a denial of service or output of specific quality parameters out of-the range can lead to catastrophic consequences in the financial sector, industry, energy sector, and so on have also increased. Modern developers of communication technologies are forced to solve several problems simultaneously and ensure not only the security of the information transmitted, but also the speed to transfer large amounts of data. In [5], the authors propose to use a McEliece cryptosystem in the Sequitur software, which allows integrally solve the problems of performance and security while transmitting sensitive information. In [6], the McEliece cryptosystem is used as a mechanism to ensure integrity in the stegosystem that provides storage information about the artist, lyrics and performance in MPEG Layer-III or MP3 file. The cryptosystem is used to store both personal (private), and public key in the ID3v2 tag format. In [7, 8], it is proposed to use the McEliece cryptosystem for solving authentication (authenticity) problems and forming a digital signature based on algebraic coding theory, as well as for the transmission of confidential (medical) information). The authors of [9] propose to use the McEliece cryptosystem in the Secure Key Management software (SKM, a framework with a high degree of scalability relative to memory), to generate key sequences and their distribution.

To reduce the cost of transmission and processing of data, ensure the required performance and reliability of the information secrecy (security), it is proposed to use asymmetric crypto-code systems on the McEliece theoretical code scheme [10–12]. In [13, 14], the basic principles and mathematical models of asymmetric crypto-code systems construction based on the McEliece and Niederreiter theoretical-code schemes (TCS) on elliptic codes that allow integrally provide the required reliability performance of information secrecy and data transmission speed in communication systems are considered. At the same time the analysis of asymmetric crypto-code system software implementation on the Niederreiter theoretical code scheme (TCS) [15] showed significant implementation complexity that makes it difficult to use theoretical code schemes for the construction of asymmetric cryptographically strong systems. In [16], the new approaches to breaking the McEliece cryptosystem based on randomized concatenated codes are considered. Development of modified crypto-code systems using modified algebraic codes is a perspective direction in solving these scientific and technical problems.

3. The aims and objectives of the study

The objective is to analyze the overall design of construction of theoretical code schemes as an integrated mechanism for providing the reliability, efficiency and safety in general data processing cycle. To achieve the goal, are considered the following tasks are considered:

– to analyze the overall structure of asymmetric crypto-code system constructing (ACCS), to assess the effectiveness and performance compared to the symmetric and asymmetric cryptographic algorithms;

– to consider the mathematical model and basic algorithms of information transfer in the McEliece ACCS on shortened codes;

– to analyze the costs of software implementation of crypto-code means of information security based on the McEliece TCS.

4. The general construction of the theoretical-code schemes, evaluation of their effectiveness as compared to other cryptographic methods

Let us consider the overall design of theoretical code schemes. We fix a finite field GF(q). Let us consider the vector space $GF^n(q)$ as a set of n-sequences of elements of GF(q) with component wise addition and multiplication by a scalar. Linear (n, k, d) code C is a subspace in $GF^n(q)$, i. e. a non-empty set of n-sequences (code words) over GF(q), k – the linear subspace dimension, d – minimum code distance (minimum weight of a non-zero codeword).

The main purpose of information encryption is to control (detect and correct) errors that occurred when sending a message through a channel with noise. For error control, the encoder introduces redundancy (checked part of the length r, r=n–k) in the transmitted data. On the receiving side, analyzing the properties of the test part and its correspondence to the transmitted data, the decoder reduces the effects of errors occurring during transmission.

The decoding problem can be effectively solved (with polynomial complexity) for a narrow class of codes, such as Bose-Chaudhuri-Hocquenghem error-correcting codes (BCH) and Reed-Solomon codes. One of the most effective algorithms for BCH codes algebraic decoding is the Berlekamp-Massey algorithm and its modifications (improvements). It is well known [17–20] that the Berlekamp-Massey algorithm contains the number of implementation of multiplications, order t^2, or, formally, the complexity of the algorithm $O(t^2)$, where t – correcting capability of the code, $t=\lfloor(d-1)/2\rfloor$. For a big t, an accelerated Berlekamp-Massey algorithm, which allows to reduce the computational complexity of the algorithm is used. The recursive Berlekamp-Massey algorithm is even more effective in terms of computational complexity. The asymptotic complexity of decoding the Reed-Solomon codes in this case does not exceed $O(n\log^2 n)$, and is very close to the value $O(n\log n)$.

The decoding of an arbitrary linear code (generic code) is a very complicated computational task, the complexity of its solution increases exponentially. Thus, for correlation decoding of random (n, k, d) code over GF(q), it is necessary, in general, to compare the received sequence with all q^k code words and select the closest (in the Hamming metric). Even for small n, k, d and q, the correlation decoding task is very labor-intensive. This provision forms the basis of all cryptographic systems on algebraic block codes. By disguising a code with fast decoding algorithm (polynomial complexity) as an arbitrary (random) linear code, the decoding task for an outside observer (an attacker) can be represented as a computational task (with exponential complexity).

For the authorized user of a cryptosystem (having a secret key), the decoding is a polynomially solvable problem. General classification of theoretical code schemes is shown in Fig. 1.

To ensure security in modern communication systems, symmetric and asymmetric cryptographic algorithms, providing the required cryptographic strength are generally used. As the analysis shows, the use of theoretical code scheme allows fast cryptographic transformation providing provable strength (Table 1). The complexity of their implementation is comparable with symmetric crypto algorithms with block symmetric ciphers (BSC). Moreover, their practical application allows using a public key infrastructure and building integrated mechanisms for cryptographic data transformation and channel coding for the complex security and reliability of data transmission.

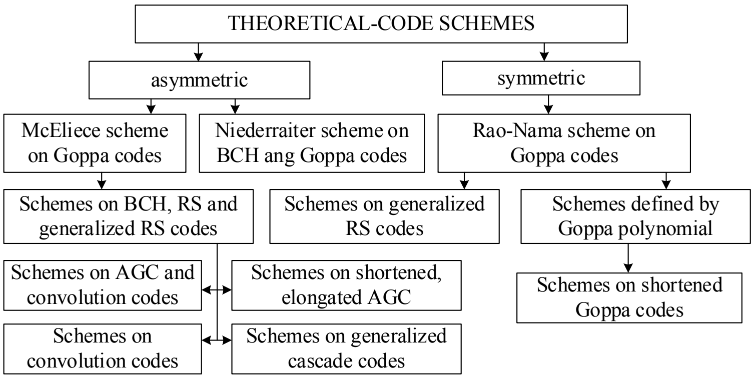

THEORETICAL-CODE SCHEMES
asymmetric
symmetric
McEliece scheme on Goppa codes
Niederraiter scheme on BCH ang Goppa codes
Rao-Nama scheme on Goppa codes
Schemes on BCH, RS and generalized RS codes
Schemes on generalized RS codes
Schemes defined by Goppa polynomial
Schemes on AGC and convolution codes
Schemes on shortened, elongated AGC
Schemes on shortened Goppa codes
Schemes on convolution codes
Schemes on generalized cascade codes

Fig. 1. General theoretical-code classification

Table 1 shows the results of comparative studies of cryptographic methods effectiveness of information protection with a fixed level of strength:

– middle (cryptanalysis complexity with the well-known algorithm is not less than 2^{128} operations);

– high (cryptanalysis complexity with the well-known algorithm is not less than 2^{256} operations);

– very-high (cryptanalysis complexity with the well-known algorithm is not less than 2^{512} operations).

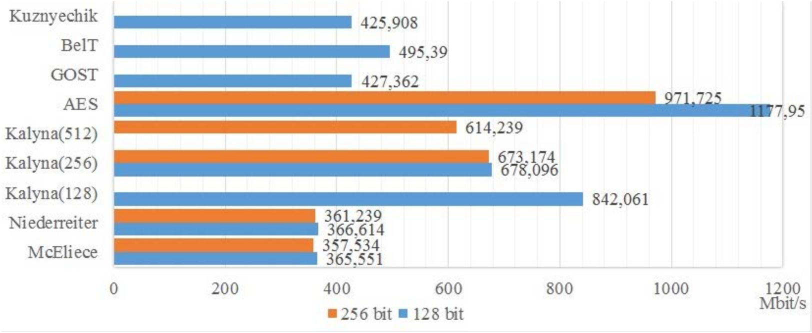


Fig. 2. Evaluation of cryptographic conversion performance in BSC and ACCS

Table 1

The results of comparative studies of cryptographic methods effectiveness of information protection with a fixed level of strength

Cryptographic transformation methods	Security model	Key data length, bits	Encryption speed, bits/s	Additional functions
Block symmetric ciphers	Practical security	128, 256, 512	10^6–10^9	–
Stream symmetric ciphers	Practical security	128, 256, 512	10^7–10^{10}	–
RSA-like cryptalgorithms	Provable security	3248 (128), 15424 (256)	10^2–10^3	–
Asymmetric cryptalgorithms on elliptic curves	Provable security	283 (128), 571 (256)	10^3–10^4	–
ACCS	Provable security	$0.5{\cdot}10^6$, (128), $2{\cdot}10^6$ (256)	10^6–10^8	Error control, reliability provision

Evaluation results of data conversion algorithms performance in symmetric ciphers and ACCS are shown in Fig. 2.

Thus, as follows from the given results of a comparative analysis, asymmetric crypto algorithms; with the use of theoretical-code schemes allow you to implement cryptographic information protection according to the public-key technology and thus provide the speed of crypto-code information conversion with the speed of block symmetric ciphers encryption. Furthermore, the practical use of theoretical-code means of information protection provides security and reliability of transmitted data based on the integration of the channel coding and encryption mechanisms. Hence, the use of theoretical-code schemes on the one hand is more economically advantageous than the use of a whole range of different encryption and channel coding mechanisms, solving individual problems, but on the other – there is a significant reduction in the total computational cost per unit of processed and transmitted information, i. e., reduced processing time increases data transmission efficiency. Let us consider the mathematical model and basic algorithms of the McEliece ACCS.

5. Mathematical model and basic algorithms of information conversion in the proposed McEliece system on shortened codes

Known methods for the modification of linear block codes are more fully discussed in [17–20]. Fig. 3 shows the most common modification methods.

Lengthening (n, k, d) of linear block code is to increase the length of n+x by adding new information symbols k+x. Extension (n, k, d) of linear block code is to increase the length of n+x by adding new check symbols r+x. Puncturing (n, k, d) of linear block code is to reduce the length of n–x by decreasing of check symbols r–x. Shortening (n, k, d) of linear block code is to reduce the length of n–x by decreasing of information symbols k–x. Augmentation (n, k, d) of linear block code is to increase the length of k+x information symbols without increasing the code length. Expurgation (n, k, d) of linear block code is to reduce the k–x information symbols without code length increasing.

Potential strength of theoretical code schemes is defined by the complexity of decoding the random (n, k, d) block code. Hence, for the construction of potentially persistent theoretical code schemes, modification techniques that do not allow reducing the minimum code distance should be used. Methods of lengthening and shortening of the linear block codes do not change the minimum distance and, therefore, allow us to construct asymmetric crypto-code systems resistant to breaking.

The simplest and most convenient method of modifying a linear block code, not reducing the minimum code distance is shortening its length by reducing the information symbols. Let I=(I_1, I_2, ..., I_k) – information vector (n, k, d) of block code. We chose a subset h of information symbols, |h|=x, x≤1/2k. We put zeros in the information vector I in the subset h, i. e. $I_i=0, \forall I_i \in h$. On the other positions of the vector I, we place the information symbols. While the information vector encoding, the symbols of the set h are not involved (they are null) and can be discarded, and the resulting code word is shorter by x code symbols. For modification (shortening) of elliptic codes, we use the reduced set of the curve points. The following statement is true.

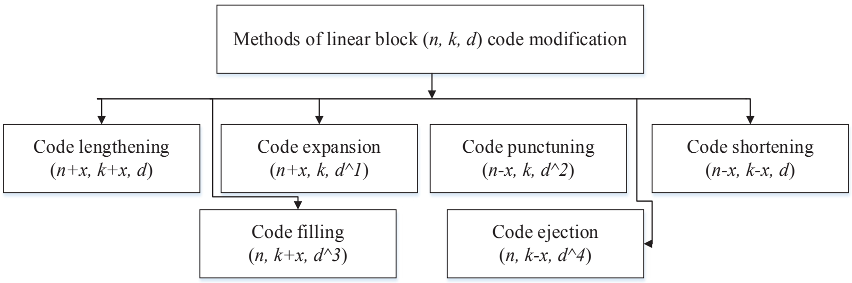

Methods of linear block (*n, k, d*) code modification
Code lengthening (*n*+*x, k*+*x, d*)
Code expansion (*n*+*x, k, d^1*)
Code punctuning (*n-x, k, d^2*)
Code shortening (*n-x, k-x, d*)
Code filling (*n, k*+*x, d^3*)
Code ejection (*n, k-x, d^4*)

Fig. 3. Means of linear block codes modification

Statement 1. Let EC – an elliptic curve over GF(q), g=g(EC) – the curve genus, EC(GF(q)) – a set of its points over a finite field, N=EC(GF(q)) – their number. Let X and h – nonintersecting subsets of points, X∪h=EC(GF(q)), |h|=x. Then shortened elliptic (n, k, d) code over GF(q), built through mapping like $\varphi: X \to P^{k-1}$, is linked by characteristics k+d≥n, where:

$$n = 2\sqrt{q} + q + 1 - x,$$

$$k \geq \alpha - x,$$

$$d \geq n - \alpha,\ \alpha = 3 \times \deg F. \qquad (1)$$

Statement 2. Shortened elliptic (n, k, d) code over GF(q), built through mapping like $\varphi: X \to P^{r-1}$, is linked by characteristics *k*+*d*≥*n*, where:

$$n = 2\sqrt{q} + q + 1 - x,$$

$$k \geq n - \alpha,$$

$$d \geq \alpha,\ \alpha = 3 \times \deg F. \qquad (2)$$

Using the result of Statements 1, 2, we set the theoretical-code scheme on modified elliptic codes, built through mapping like $\varphi: X \to P^{k-1}$ and $\varphi: X \to P^{r-1}$. The following statements are true.

Statement 3. Shortened elliptic (n, k, d) code over GF(2^m), built through mapping like $\varphi: X \to P^{k-1}$, defines the modified theoretical-code scheme with the following parameters:

$$l_{K+} = x \cdot \left\lceil \log_2\left(2\sqrt{q} + q + 1\right) \right\rceil; \qquad (3)$$

$$l_I = (\alpha - x) \cdot m; \qquad (4)$$

$$l_S = \left(2\sqrt{q} + q + 1 - x\right) \cdot m; \qquad (5)$$

$$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right). \qquad (6)$$

Statement 4. Shortened elliptic (n, k, d) code over GF(2^m), built through mapping like $\varphi: X \to P^{r-1}$, defines the modified theoretical-code scheme with the following parameters:

– the dimension of the secret key is determined by (3);

– the dimension of the information vector (in bits):

$$l_I = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \qquad (7)$$

– the dimension of the codegram is defined by (5);

– relative transmission rate:

$$R = \frac{2\sqrt{q} + q + 1 - \alpha}{2\sqrt{q} + q + 1 - x}. \qquad (8)$$

Let us consider the formal description of a modified asymmetric crypto-code information protection system based on the use of modification methods and practical algorithms of formation of codegrams and their decryption in the developed theoretical-code schemes.

Mathematical model of ACCS using the McEliece TCS based on shortening (reduction of information symbols) is formally defined by a combination of the following elements [9]:

– a set of plaintexts

$$M = \{M_1, M_2, \ldots, M_{q^k}\},$$

where $M_i = \{I_0, I_{h_1}, .. \ I_{h_j}, I_{k\text{-}1}\}$, $\forall I_j \in GF(q)$, h_j – information symbols equal to zero, $|h| = \frac{1}{2}k$, i. e. $I_i=0, \forall I_i \in h$;

– a set of secret texts (codegrams)

$$C = \{C_1, C_2, \ldots, C_{q^k}\},$$

where

$$C_i = (c^*_{X_0}, c^*_{h_1}, \ldots, c^*_{h_j}, c^*_{X_{n-1}}),\ \ \forall c^*_{X_j} \in GF(q);$$

– a set of direct mappings (based on public key usage – generating matrix)

$$\phi = \{\phi_1, \phi_2, \ldots, \phi_s\},$$

where

$$\phi_i : M \to C_{k-h_j},\ \ i = 1, 2, \ldots, s;$$

– a set of inverse mappings (based on secret (private) key usage – disguise matrixes)

$$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, \ldots, \phi_s^{-1}\},$$

where

$$\phi_i^{-1} : C_{k-h_j} \to M,\ \ i = 1, 2, \ldots, s;$$

– a set of keys, parameterizing direct mappings (public key of the authorized user)

$$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, \ldots, K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, \ldots, G_X^{ECs}{}_{a_i}\},$$

where $G^{ECi}_{X\ \ a_i}$ – generating $n\times k$ matrix disguised as a random code of algebra-geometric block (n, k, d) code with elements from $GF(q)$, i. e. $\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$; $i \quad 1,2,\ldots,s$; a_i – a set of polynomial curve coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of points on the curve from the space P^2.

– a set of keys, parameterizing inverse mappings (private (secret) key of the authorized user)

$$K^* = \{K_1^*, K_2^*, \ldots, K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, \ldots, \{X,P,D\}_s\},$$

$$\{X,P,D\}_i = \{X^i, P^i, D^i\},$$

where X^i – disguise nondegenerate randomly equiprobably formed by a source of keys $k\times k$ matrix with elements from GF(q); P^i – permutation randomly equiprobably formed by a source of keys $n\times n$ matrix with elements from $GF(q)$; D^i – diagonal formed by a source of keys $n\times n$ matrix with elements from $GF(q)$, i. e.

$$\phi_i^{-1} : C \xrightarrow{K_i^*} M,\ i = 1,2,\ldots,s,$$

the complexity of the inverse mapping ϕ_i^{-1} without knowing the key $K_i^* \in K^*$ is associated with solving theoretical-complexity problems in random code decoding (general position code).

The initial data in the description of the considered asymmetric crypto-code information protection system are:

– algebrogeometric block (n, k, d) code C_{k-h_j} over GF(q), i. e. a set of code words $C_i \in C_{k-h_j}$ such that the equality is true $C_i H^T = 0$, where H – check matrix of algebrogeometric block code;

– a_i – a set of the curve polynomial coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of the curve points from space P^2 to form the generating matrix;

– h_j – information symbols, equal to zero, $|h|=1/2k$, i. e. $I_i=0$, $\forall I_i \in h$;

– disguising matrix mappings, given by a set of matrices $\{X, P, D\}_i$, where X – nondegenerate $k\times k$ matrix over GF(q), P – permutation $n\times n$ matrix over GF(q) with one non-zero element in each row and each column of the matrix, D – diagonal $n\times n$ matrix over GF(q) with non-zero elements on the main diagonal.

In asymmetric crypto-code system based on the McEliece TCS, the modified (shortened) algebrogeometric (n, k, d) code C_{k-h_j} with fast decoding algorithm is disguised as a random (n, k, d) code $C_{k-h_j}{}^*$ by multiplying the generating matrix G^{EC} of the code C_{k-h_j} by the secret disguise matrices X^u, P^u and D^u [8], providing the formation of the authorized user's public key:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u,\quad u \in \{1,2,\ldots,s\},$$

where G^{EC} – generating $n\times k$ matrix of algebrogeometric block (n, k, d) code with elements from $GF(q)$, built on the basis of the user-selected curve polynomial coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of points on the curve from the space P^2.

Forming a closed text $C_j \in C_{k-h_j}$ on the basis of the entered plaintext $M_i \in M$ and a given public key $G^{ECu}_{X\ \ a_i}$, $u \in \{1,2,\ldots,s\}$ is carried out by forming a code word of the disguised code by adding a random vector $e = (e_0, e_1, \ldots, e_{n-1})$:

$$C_j = \phi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e,$$

where the Hamming weight (number of nonzero elements) of the vector does not exceed the correcting ability of the algebraic block code used:

$$0 \le w(e) \le t = \left\lfloor \frac{d \quad 1}{} \right\rfloor,$$

$\lfloor x \rfloor$ – the integer part of a real number x.

For each formed secret text $C_j \in C_{k-h_j}$, the corresponding vector $e = (e_0, e_1, \ldots, e_{n-1})$ acts as a one-time session key, i.e. for a particular E_j the vector e is generated randomly equiprobably and independently of the other closed texts.

The communication channel receives

$$C_j^* = C_j - C_{k-h_j}.$$

On the receiving side, an authorized user who knows the disguise rule, the number and location of zero information symbols can use a fast algebrogeometric code decoding algorithm (with polynomial complexity) to recover the plaintext [8]:

$$M_i = \phi_u^{-1}\left(C_j^*, \{X,P,D\}_u\right).$$

To recover the plaintext, an authorized user adds zero information symbols $C_j^* = C_j + C_{k-h_j}$, from the recovered secret text C_j, removes the effect of the secret permutation and diagonal matrices P^u and D^u:

$$\begin{aligned}
C\ \ &= C_j^* \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(M_i \cdot \left(G_X^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \\
&= \left(M_i \cdot \left(X^u \cdot G \cdot P^u \cdot D^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \\
&= M_i \cdot \left(X^u\right)^T \cdot (G)^T \cdot \left(P^u\right)^T \cdot \left(D^u\right)^T \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + \\
&+ e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = M_i \cdot \left(X^u\right)^T \cdot (G)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},
\end{aligned}$$

decodes the received vector by the Berlekamp-Massey algorithm [15]:

$$C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

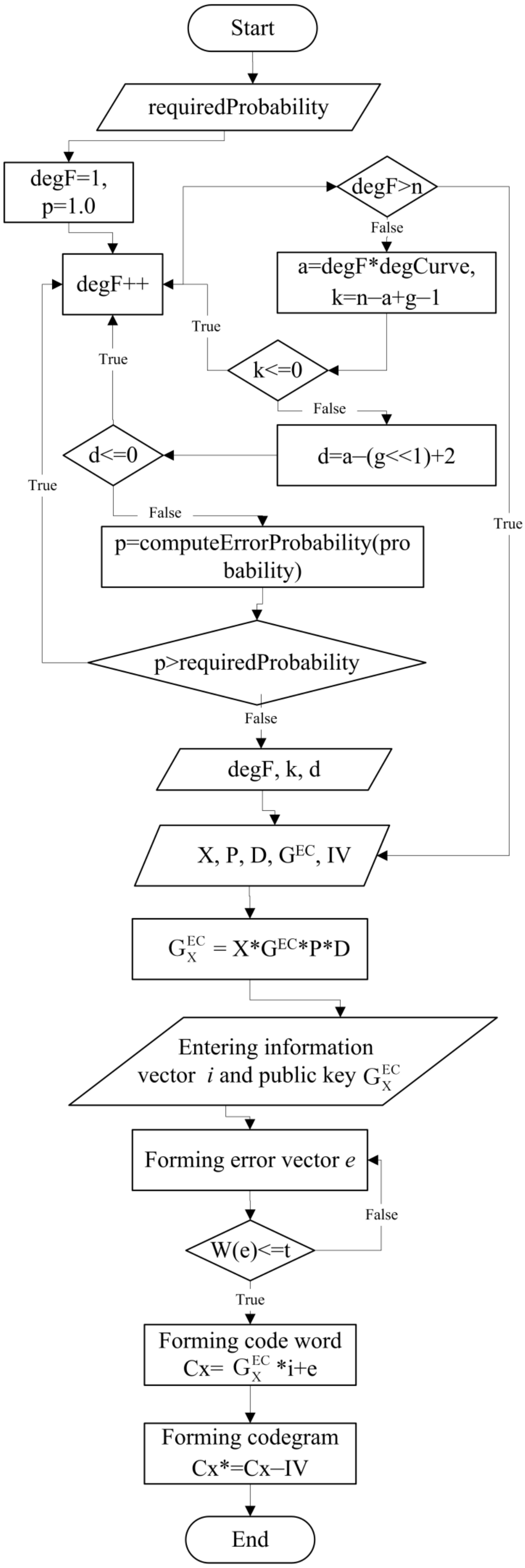
i. e. gets rid of the second term and from the multiplier $(G)^{ECT}$ in the first term in the right side of the equation, and then removes the effect of the disguise matrix X^u. For this, the result of decoding $M_i \cdot \left(X^u\right)^T$ should be multiplied by

$$\left(X^u\right)^{-1}:\ \left(M_i \cdot \left(X^u\right)^T\right) \cdot \left(X^u\right)^{-1} = M_i.$$

The resulting solution is the plain text M_i.

Let us consider the practical algorithms of formation and decryption/decoding cryptogram/codegram in a modified asymmetric crypto-code system based on the McEliece TCS on elliptic shortened codes. Fig. 4 shows an algorithm of cryptogram/codegram formation.

The algorithm of codegram formation in the modified McEliece asymmetric crypto-code system with shortened modified code is defined by a sequence of the following steps.



Stage 1. Set code parameters

requiredProbability – defined probability of block distortion;
n – total number of symbols in code (code length);
k – number of information symbols;
d – minimal distance of code combinations by Hemming;
g – curve genus;
degF – the degree of generating function;
degCurve – curve degree.

Stage 2. Forming private and public keys of asymmetric cryptosystem, entering information package

X – non-degenerate matrix *kxk* over *GF(q)*;
P – permutational matrix *nxn* over *GF(q)*;
D – diagonal matrix *nxn* over *GF(q);*
G^{EC} – check matrix *rxn* of elliptic code over *GF(q)*;
a_i – coefficients set of curve polynomial $a_1 \dots a_6$;
IV – initialization vector, *IV*=|*h*|=*1/2k*-reducing elements.

Stage 3. Forming session key and codegram

vector *e* forms randomly, equiprobably and independently from another secret texts;
communication channel receives code without zero elements of initialization vector (shortening operation)

Fig. 4. The algorithm of codegram formation in the modified McEliece ACCS with shortened modified code

Step 1. We fix a finite field GF(q). We fix an elliptic curve $y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3$ and a set of its points EC(GF(q)):(P_1, P_2, ...,P_N) over GF(q). We fix a subset of points h(GF(q)): (P_{x1}, P_{x2}, ...,P_{xx}), h⊆EC(GF(q)), |h|=x and keep it secret.

Step 2. We form the initialization vector IV=EC−h_j, h_j – information symbols equal to zero, $|h|=\frac{1}{2}k$, i. e. $I_i=0$, $\forall I_i \in h$;

Step 3. By entering the information vector I, we form the codeword c. If (n, k, d) code over GF(q) is given by its generating matrix, then c=I×G.

Step 4. We form the random vector of the error e so that w(e)≤t, $t=\lfloor (d-1)/2 \rfloor$. We add the formed vector to the code word, receive the code word: c*=c+e.

Step 5. We form the codegram by removing (shortening) the initialization vector symbols: c_X*=c^*−IV.

The algorithm of codegram decoding in modified theoretical-code schemes on elliptic codes is defined by a sequence of the following steps:

Step 1. Entering the codegram to be decoded. Entering the private key – generating and/or parity-check matrix of the elliptic code.

Step 2. Codegram – a codeword with elliptic code errors. Error vector weight w(e)≤t. We decode the codegram – find the error vector.

Step 3. We form the needed information vector.

The proposed algorithm for decoding in the modified asymmetric crypto-code system using the McEliece TCS with shortened modified code is shown in Fig. 5.

The main stage of the codegram decoding algorithm in the theoretical-code scheme on elliptic codes is decoding of the received sequence. While the codegram decoding, an authorized user should consider the shortened code parameters in the theoretical-code schemes on modified elliptic codes.

The block diagram of the real-time information exchange protocol using the asymmetric cryptosystem based on the modified McEliece TCS with modified (shortened) elliptic codes is shown in Fig. 6.

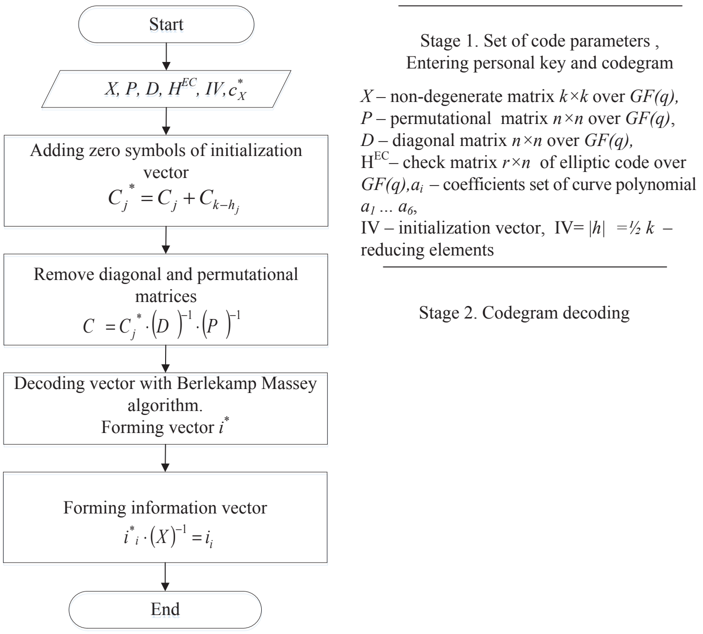

Start
$X, P, D, H^{EC}, IV, c_X^*$
Adding zero symbols of initialization vector
$C_j^* = C_j + C_{k-h_j}$
Remove diagonal and permutational matrices
$C = C_j^* \cdot (D)^{-1} \cdot (P)^{-1}$
Decoding vector with Berlekamp Massey algorithm.
Forming vector i^*
Forming information vector
$i^*_i \cdot (X)^{-1} = i_i$
End
Stage 1. Set of code parameters , Entering personal key and codegram
X – non-degenerate matrix $k\times k$ over $GF(q)$,
P – permutational matrix $n\times n$ over $GF(q)$,
D – diagonal matrix $n\times n$ over $GF(q)$,
H^{EC}– check matrix $r\times n$ of elliptic code over $GF(q)$,a_i – coefficients set of curve polynomial $a_1 \dots a_6$,
IV – initialization vector, IV= |h| =½ k – reducing elements
Stage 2. Codegram decoding

Fig. 5. Algorithm in the modified McEliece ACCS with shortened modified code

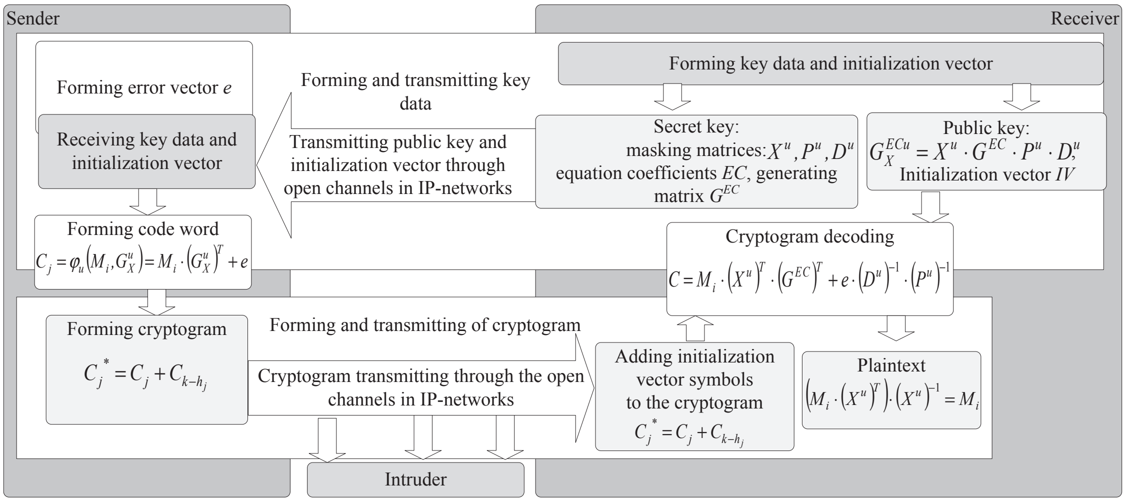

Sender
Receiver
Forming error vector e
Forming and transmitting key data
Forming key data and initialization vector
Receiving key data and initialization vector
Transmitting public key and initialization vector through open channels in IP-networks
Secret key: masking matrices:X^u, P^u, D^u equation coefficients EC, generating matrix G^{EC}
Public key: $G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u_,$ Initialization vector IV
Forming code word
$C_j = \varphi_u(M_i, G_X^u) = M_i \cdot (G_X^u)^T + e$
Cryptogram decoding
$C = M_i \cdot (X^u)^T \cdot (G^{EC})^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}$
Forming cryptogram
$C_j^* = C_j + C_{k-h_j}$
Forming and transmitting of cryptogram
Cryptogram transmitting through the open channels in IP-networks
Adding initialization vector symbols to the cryptogram
$C_j^* = C_j + C_{k-h_j}$
Plaintext
$(M_i \cdot (X^u)^T) \cdot (X^u)^{-1} = M_i$
Intruder

Fig. 6. Real-time information exchange protocol using the asymmetric cryptosystem based on the modified McEliece TCS with modified (shortened) elliptic codes

Let us investigate the software implementation energy costs of crypt-code means of information security based on the McEliece TCS on modified (shortened) elliptic codes.

6. Estimation of energy costs of software implementation of the proposed McEliece system

To estimate time and speed parameters, it is common to use the unit of measurement cpb, where cpb (cycles per byte) – the number of processor cycles, which should be spent to process 1 byte of incoming information. Algorithm complexity is computed by the expression:

$$\text{Per} = \text{Utl} * \text{CPU\_clock} / \text{Rate},$$

where Utl – utilization of the CPU core (%); Rate – algorithm bandwidth (bytes/sec).

Table 2 shows the dependence of the code sequence length of the algebrogeometric code in the McEliece and Niederreiter TCS on the number of CPU cycles to perform elementary operations in the software implementation of crypto-code systems.

Table 3 shows the investigation results for evaluating time and speed parameters of procedures of forming and decoding information in the asymmetric crypto-code system based on the McEliece TCS.

The analysis (Tables 2, 3) enables to conclude about significant energy cost when implementing asymmetric crypto-code systems in the protocols of communication systems and technologies, which greatly complicates their use. To eliminate the disadvantage, it is proposed to use the modified asymmetric crypto-code schemes based on the usage of error-correcting code, which provides decrease of energy costs and users key data volumes by storage of information about coefficients of an elliptic curve in an affine space to build the corresponding matrices (private and public keys).

Table 2

The dependence of the code sequence length in the McEliece ACCS and modified ACCS on the number of CPU cycles

Code sequence length		McEliece on shortened codes			McEliece		
		10	100	1000	10	100	1000
The number of function calls realizing elementary operations	Symbol reading	10 294 397	28 750 457	76 759 874	11 018 042	30 800 328	80 859 933
	String comparing	3 406 921	9 246 748	25 478 498	3 663 356	10 199 898	26 364 634
	String concatenation	1 705 544	5 045 748	12 379 422	1 834 983	5 125 564	13 415 329
Sum		15 406 862	43 042 953	114 617 794	16 516 381	46 125 790	120 639 896
Duration of executing functions in processor cycles *	Symbol reading	295 374	810 478	2 001 167	297 487	831 609	2 183 218
	String comparing	178 814	531 379	1 248 684	197 821	550 794	1 423 690
	String concatenation	544 990	1 328 114	3 586 486	544 990	1 522 293	3 984 353
Sum		1 006 781	2 749 548	7 247 488	1 040 298	2 904 696	7 591 261
Duration of executing ** in msec		0.52	1.37	3.4	0.55	1.53	4

*Note: * – duration of 1000 operations in processor cycles: symbol reading – 27 cycles, string comparing – 54 cycles, string concatenation – 297 cycles; ** – the processor with a clock speed of 2 GHz taking into account operating system loading of 5 % was taken for the calculation*

Table 3

The investigation results for evaluating time and speed parameters of procedures of forming and decoding information in the asymmetric crypto-code system based on the McEliece TCS

Parameters	Code sequence length	Algorithm bandwidth, Rate (byte/sec)	Utilization of the processor core, (%)	Algorithm complexity, Per (cpb)
The number of function calls that implement the basic operations	100	46 125 790	56	61.5
	1000	120 639 896	56	62.0

7. Conclusions

1. The overall structure of asymmetric crypto-code systems based on the McEliece TCS enabling integrated (with a single device) provision of the required indicators of reliability, efficiency and data security was analyzed. A major shortcoming of ACCS based on the McEliece TCS is a big volume of key data, that constricts their use in different communication system areas (today cryptographic strength on the level of the provable strength model is provided while building ACCS in the Galois field GF(2^{13})). The use of modified (shortened) elliptic (algebraic) codes helps to reduce the volume of key data, while maintaining the requirements for cryptographic strength of ACCS. Estimation the data conversion performance is comparable to the speed of direct and inverse cryptographic conversion of modern BSC, this ensures the cryptographic strength at the level of asymmetric cryptosystems (cryptographic strength is based on the theoretical complexity problem – random code decoding).

2. The proposed mathematical model, practical algorithms for encryption/decryption and coding/decoding of cryptograms/codegrams in the developed modified crypto-code system based on the McEliece TCS allows to realize encryption/decryption at speeds of symmetric cryptosystems with BSC. The complexity of the codegram forming and decoding is determined, accordingly, by encoding/decoding complexity of modified (shortened) elliptic codes and polynomially depends on the code length and correcting dependency. For 100 bytes of transmitted data, the Per algorithm complexity is 61.5 cpb, and for 1000 bytes is 62 cpb, that does not affect the complexity of the algorithm with a significant increase in data to be processed.

3. Transferring a key sequence using the modified McEliece ACCS based on the shortened code allows to use open channels of communication systems for the transmission of confidential information and integrally provide the required indicators of reliability and efficiency of the entire data processing cycle.

References

1. Semenov, S. G. Modeli i metody upravleniya setevymi resursami v informatsionno-telekommunikatsionnykh sistemakh [Text]: monografiya / S. G. Semenov, A. A. Smirnov, E. V. Meleshko. – Kharkov: NTU "KhPI", 2011. – 212 p.
2. Rzaev, H. N. Analiz sostojanija i putej sovershenstvovanija protokolov bezopasnosti sovremennyh telekommunikacionnyh setej [Text]: monografija / H. N. Rzaev, O. G. Korol'; V. S. Ponomarenko (Ed.) // Informacionnye tehnologii v upravlenii, obrazovanii, nauke i promyshlennosti. – Kharkov: Izdatel' Rozhko S. G., 2016. – P. 217–234.
3. Telekommunikacionnye uslugi v mirovoj jekonomike [Electronic resource]. – Available at: http://www.gumer.info/bibliotek_Buks/Econom/world_econom/30.php
4. Korol', O. G. Protokoly bezopasnosti telekommunikacionnyh setej [Text] / O. G. Korol' // Sistemi obrobki informacii. – 2012. – Issue 6 (104). – P. 113–120.
5. Ojha, D. B. Transmission of Picturesque content with Code Base Cryptosystem [Text] / D. B. Ojha, A. Sharma, A. Dwivedi, B. Kumar, A. Kumar // International Journal of Computer Technology and Applications. – 2011. – Vol. 02, Issue 01. – P. 127–131. – Available at: https://doaj.org/article/6714b60516cc4aa79e56d0c421febaf3
6. Salman, A. G. Steganography application program using the ID3v2 in the MP3 audio file on mobile phone [Text] / A. G. Salman // Journal of Computer Science. – 2014. – Vol. 10, Issue 7. – P. 1249–1252. doi: 10.3844/jcssp.2014.1249.1252
7. Ojha, D. B. Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel [Text] / D. B. Ojha, A. Sharma, A. D. N. Pandey, A. Kumar // International Journal of Engineering Science and Technology. – 2010. – Vol. 2, Issue 12. – P. 7112–7117. – Available at: https://doaj.org/article/5c7da3a1e3ec4f83b552199034bd3241
8. Ojha, D. B. An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel [Text] / D. B. Ojha, A. Sharma // International Journal of Advanced Networking and Applications. – 2011. – Vol. 2, Issue 5. – P. 841–845. – Available at: https://doaj.org/article/39a3ac65d5b24b348f069dfc82eb6248
9. Jeeva, Y. C. A Novel Approach For Information Security In Ad Hoc Networks Through Secure Key Management [Text] / Y. C. Jeeva // Journal of Computer Science. – 2013. – Vol. 9, Issue 11. – P. 1556–1565. – Available at: https://doaj.org/article/378b88837cdf4cab9f8010a38a6aeb2b
10. McEliece, R. J. A Public-Key Criptosystem Based on Algebraic Theory [Text] / R. J. McEliece // DGN Progres Report 42-44. – Pasadena, C.A., 1978. – P. 114–116.
11. Niederreiter, H. Knapsack-Type Cryptosystems and Algebraic Coding Theory [Text] / H. Niederreiter // Problems of Control and Information Theory. – 1986. –Vol. 15, Issue 2. – P. 159–166.
12. Sidel'nikov, V. M. Kriptografija i teorija kodirovanija [Text]: konferencya / V. M. Sidel'nikov // Moskovskij universitet i razvitie kriptografii v Rossii. – Moscow, 2002. – 22 p.
13. Evseev, S. P. Issledovanie teoretiko-kodovyh shem dlja kompleksnogo obespechenija bezopasnosti i dostovernosti dannyh v informacionnyh sistemah [Text] / S. P. Evseev, B. P. Tomashevskij // Naukovij visnik Chernivec'-kogo universitetu. Serija: Komp'juterni sistemi ta komponenti. – 2011. – Vol. 2, Issue 1. – P. 6–14.
14. Rzaev, H. N. Matematicheskie modeli kripto-kodovyh sredstv zashhity informacii na osnove TKS [Text] / H. N. Rzaev, G. G. Iskenderzade, F. G. Samedov, Z. B. Imanova, Zh. S. Dzhamalova // Zashhita informacii. – Kiev: NAU, 2016. – Issue 23. – P. 24–26.
15. Rzaev, H. N. Analiz programmnoj realizacii metoda nedvoichnogo ravnovesnogo kodirovanija [Text] / H. N. Rzaev, A. S. Cyganenko // Azərbaycan Texniki Unuversiteti, Elmi Əsərlər Cild. – 2016. – Issue 1. – P. 107–112.
16. Hamdi, O. On the Usage of Chained Codes in Cryptography [Text] / O. Hamdi // International Journal of Computer Science and Security. – 2010. – Vol. 3, Issue 6. – P. 482–490. – Available at: https://doaj.org/article/c0f40bdb1f6149f4ac107d44a95c9531
17. Blejhut, R. Teorija i praktika kodov, kontrolirujushhih oshibki [Text] / R. Blejhut. – Moscow: Mir, 1986. – 576 p.
18. Klark, Dzh.-ml. Kodirovanie s ispravleniem oshibok v sistemah cifrovoj svjazi [Text] / Dzh.-ml. Klark; B. S. Cybakov (Ed.). – Moscow: Radio i svjaz', 1987. – 392 p.
19. Mak-Vil'jams, F. Dzh. Teorija kodov, ispravljajushhih oshibki [Text] / F. Dzh. Mak-Vil'jams, N. Dzh. A. Slojen. – Moscow: Svjaz', 1979. – 744 p.
20. Muter, V. M. Osnovy pomehoustojchivoj teleperedachi informacii [Text] / V. M. Muter. – Leningrad: Jenergoatomizdat. Leningr. otd-nie, 1990. – 288 p.
21. Kasami, T. Teorija kodirovanija [Text] / T. Kasami, N. Tokura, E. Ivadari, Ja. Inagaki; B. S. Cybakov, S. I. Gel'fand (Eds.). – Moscow: Mir, 1978. – 576 p.
22. Kuznecov, O. O. Zahist informacii ta ekonomichna bezpeka pidpriemstva [Text]: monografija / O. O. Kuznecov, S. P. Evseev, S. V. Kavun. – Kharkov: Vid. HNEU, 2008. – 360 p.