Training of Cryptography as a Way of Developing System Thinking at Secondary School Students

Iskandar Azhmukhamedov
Astrakhan State University
Astrakhan, Russia, 414056
iskander_agm@mail.ru

Valentina Kuznetsova
Astrakhan State University
Astrakhan, Russia, 414056
arhelia@bk.ru

Olga Vybornova
Astrakhan State University
Astrakhan, Russia, 414056
olga.vyb.90@gmail.com

Abstract

The article deals with domestic and foreign experience in the introduction of cryptography as an element of secondary education. The authors analyzed current methods of teaching cryptography for students. They concluded that there are no comprehensive methodological and didactic materials for conducting classes with schoolchildren. The authors proposed their own elective course, based on the system–activity approach and elements of project teaching. The article shows the effect of the methodology using the author's software for the developing of students' systems thinking.

Keywords: cryptography, basic education, elective course, teaching cryptography, system thinking, illustrative software

1 Introduction

Cryptographic methods of protecting information have recently become the basis for ensuring information security in almost all areas of public life: military, social, economic, etc. In this regard, there is a constant need for an influx of young talented personnel in this field of science. They could give a new impulse to its development, as well as provide a connection of cryptography with other areas of knowledge.

For this purpose, potential specialists should have a spacious mind and deep systems thinking. Learning the basics of cryptography in primary school contributes to the development of the present type of thinking. According to psychologists, this effect is based on the fact, that cryptography classes develop child logic, the ability to link certain features to an integrated system, to see and notice certain essential elements. For example, as regards complex encryption, when cryptographer uses several types of encryption, it is necessary to be able to distinguish features of various encryption methods.

Children's interest in solving various kinds of riddles appears even in preschool age. Despite this fact, specific steps for the official introduction of cryptography into the school curriculum in Russia were not taken, although there have been some attempts to teach this subject in an optional way [Vas04]; [Bos 13]; [Dus17].

In: Jože Rugelj, Maria Lapina (eds.): Proceedings of SLET-2019 – International Scientic Conference Innovative Approaches to the Application of Digital Technologies in Education and Research, Stavropol – Dombay, Russia, 20-23 May 2019, published at http://ceur-ws.org

2 Task

In this regard, it is necessary to develop a methodology and specialized teaching and demonstration software for early training of schoolchildren in the basics of cryptographic information protection. It is the purpose of this work.

3 Development of methodology

At the first stage of the creation of the mentioned methodology, it is necessary to analyze the existing domestic and foreign experience in teaching cryptography at school, to identify general trends and identify main differences in educational approaches.

3.1 Domestic experience

In domestic educational practice, some issues related to cryptography are partially considered within the school course of computer science in the study of topics related to coding. There is no special cryptography course as a separate subject within the federal educational standard and approximate educational programs.

Issues related to cryptography, according to the course schedule, are usually discussed in the textbooks of the following classes.

In programs of the 2nd, 3rd, 5th grades (according to the textbooks by N.V. Matveeva), pupils are taught encryption using the example of Caesar cipher along with binary encoding, while students are not given an explanation of the difference between these concepts [Mat16]. As a result, in the minds of pupils, encryption becomes identical to coding, which is wrong. For example, Morse code, being a world–famous method of character coding, provides the convenience of transmitting information over communication lines, while cryptoalgorithms serve to ensure the confidentiality of stored and transmitted information.

In the 5th–grade textbook the author L.L. Bosova [Bos13] proposes to solve problems related to data encryption with students, – the example of Caesar, Gronsfeld and Atbash ciphers, – when studying the topic “Coding” in a lesson and calendar–thematic planning. Using the 5th grade textbook, teachers develop additional lessons based on detective stories. In particular, they use the works of A.C. Doyle in order to interest students in solving various ciphers.

In the 6th and 7th–grades, the tasks are similar, but their encryption is considered as one of the processes in the information system. At the same time, some teachers set “to teach how to distinguish concepts of coding and encryption of information” as one of the tasks [Azi19].

In the 10th grade textbooks (in–depth study) [Sem16] in the section “Information processes in systems” the author I.G. Semakin, among the information security measures, gives an overview of cryptography as a science, briefly describes the history of the development of cryptography, mentions asymmetric encryption for the introduction of the term “digital signature”. Also he gives the definition of the private key in symmetric cryptosystems (identifying it with the key of symmetric encryption), but this is inaccuracy and misleads students. The concept of a private key should be correctly used only when discussing asymmetric cryptosystems. To consolidate learned material in the list of practical works, there is the topic “Data Encryption”, where students need to solve problems related to Caesar and Vigenere ciphers, unnamed transposition ciphers that were not considered in the theoretical material. Here authors–compilers erroneously use the term “decoding” in the meaning of “decryption”. Also, students are invited to come up with their own cipher in a practical task.

In the 11th–grade textbook, the question of cryptography is included in the lesson “Organization of information security. Antivirus protection of information” (program based on textbooks by I.G. Semakin – in–depth level). By analogy with the 10th–grade textbook, the author makes an error in identifying encryption and encoding. He defines: “encryption is a special type of encoding”. The definitions of cryptanalysis and encryption keys are also introduced. The paragraph has a detailed description of the Caesar cipher and encryption mechanism of the Vigenere method. To consolidate the material students are asked to solve 6 tasks for both encryption methods.

Cryptography in schools is usually not included in the educational program and left as elements of extracurricular activities – electives and clubs. The publishing house ”Binom” in 2014 offered teachers to organize extracurricular activities based on the teaching and methodic complexes proposed by them. One of them is a textbook by E.V. Tanova “Introduction to cryptography: how to protect your letter against curious people” [Tan05]. The author has developed an elective course with a detailed work program, teaching materials and a book for a student and a teacher. And she considers studying of cryptography in school at various levels in more detail in her dissertation work [Tan07].

The teacher's book includes not only themes of pre–computer ciphers, but also affects modern encryption methods (AES, DES, GOST), digital signature algorithm, key distribution algorithm. The mathematical basis of cryptographic protection of information (combinatorics, key generation) is considered in detail, but little attention is paid to the elementary symmetric transposition and substitution ciphers. As regards the first type, magic squares and grids are considered; as for the second type, the Caesar cipher, Atbash, Vigenere and a one–time notebook are considered.

Entertaining and educational books on cryptography for children also periodically appear on sale. For example, R. Dushkin "Ciphers and Quests: Mysterious Stories in Logic Riddles" [Dus17].

On the pedagogical portals, teachers attempt to develop the author's work programs for elective courses. For example, I.P. Vasilego, a teacher at Orenburg State University, has developed a handbook on cryptography for pupils, but unfortunately, there is no methodical information in it [Vas04]. Another program was proposed by the teacher of the Orenburg Presidential Cadet School A.V. Evlampyev. His methodical work presents guidelines and curriculum for the elective course on cryptography for the 9th grade. It includes the selection of content, forms of study, control of knowledge and it is aimed at assisting students in choosing a profile for studying in high school, in direction of students into the necessary field of activity today – digital technologies and information security. The structure of the elective course reflects the history and trends in the development of cryptography and its tasks, includes an overview of several symmetric and asymmetric systems [Evl19].

Most often cryptography issues are elements of electives and clubs in computer science and computer security for specialized classes. For example, the program of the elective course "Information security" for the 10th–grade in the Academic Lyceum of Tomsk, along with issues of information security of computer systems and basic concepts, includes topics on symmetric encryption and hashing algorithms (in total – 6 hours).

As for the rest, currently the passion for cryptography is encouraged and stimulated with the help of a few centers of additional education. For example, in the Astrakhan region, a club for secondary school students is organized by the Regional School Technopark. University professors are invited to classes with students. A similar elective course on cryptography, focused on grades 7–9, is implemented by Lyceum No. 8 in Orenburg.

The leaders in preparing schoolchildren for cryptography competitions are not only schools in Moscow and St. Petersburg. For example, in 2002, the Far Eastern Regional Training and Research Center on Information Security Problems was established in the Far East. This Center holds regional conferences, seminars and meetings, competitions and cryptography contests for interested teenagers.

The Organizing Committee of the Interregional Olympiad in Mathematics and Cryptography for Schoolchildren, with the support of the Academy of the Federal Security Service of Russia and the Academy of Cryptography of the Russian Federation, offers to prepare for the competitions a stingy presentation on the main types of ciphers, but does not accompany it with guidelines and explanations [ISOC].

Thus, it must be stated that there are no comprehensive methodological and didactic materials for conducting classes with schoolchildren. Each teacher selects the material for a particular cipher depending on his preferences, focusing solely on his or her own preferences or experience.

3.2 Foreign experience

Abroad, the process of integrating cryptography into the school curriculum is more successful. For example, in the Montessori system, it is believed that a child should be taught simple ciphers even before school, starting at 3 years of age.

As part of American education, cryptography is included as the elective compulsory course in middle and high school. In 2009, a team at the University of Illinois in Chicago developed a cryptography and cryptanalysis curriculum for students. This project won a grant of $ 2.5 million to ensure that cryptography was introduced into the education system within five years.

The book and course materials were initially tested in public schools in Chicago, as well as in the suburban schools of Naperville, Oak Park and La Grange. Then the pilot project was expanded to school districts across the country. So the project "Cryptoclub" was created [Bei06]. It was joined by students related to information security. Teaching on ready training materials, and the development of new ones began. "CryptoClub" Cipher Handbook became the main training course textbook. The authors of this textbook also wrote the manual "Number Theory for Future High School Teachers" with the support of the Mathematical Association of America

[Sau08]. It's important to mention the efforts of the Mathematical and Scientific Education Consortium (MSEC) and the Department of Mathematical Sciences at the University of New Mexico (NMSU), headed by Dr. Reinhard Laubenbacher, who developed cryptographic resources for teachers.

In addition, middle school teachers in the United States, along with their Russian colleagues, attempt to popularize cryptography and contribute consideration of the most popular ciphers to math learning. Such ideas are implemented in schools of the states Colorado, Idaho, Arizona and several other states [Bry17].

In 2012 faculty of RWTH Aachen University (Germany) have represented methodical materials, which have been provided by the two–day cryptography elective under the 4th international computer education conference, Porto (Portugal). This elective course is part of a great integral additional education course, the main goal of which is drawing the attention of schoolchildren to the technical sciences and developing a strong interest in them [Ber12]. The main idea of the developed course lays in the process of giving the important first glimpse of the fascinating cryptography world to secondary school students. During the course groups of three–five students independently but under the supervision of a professional pedagogue study four different cryptography algorithms: scytale cipher, Cardan grille, Caesar shift and Vigenere encryption algorithm. The first and main feature of that experience is that authors invite 11–14 years old students with quite different preparation levels. The focus stays on getting useful information and knowledge by students not only from pedagogues but from communication with each other. The second feature is that students have an opportunity to work with different assimilation level materials. That's why methodical materials of that elective course can be easily used for individual learning too. Also, a special software product has been developed for training and demonstration purposes as a support tool for the elective course. Developed product vividly illustrates difficulty for understanding cryptography transformations methods as a fascinating game.

The authors write that the course, developed in accordance with the didactic principle of search training and the system–activity approach, has already been tested in control groups. It is noted that cryptography has caused the greatest interest in girls (72% against 28% of male participants). The participants of the experiment spoke positively about group work and project work. In addition, it was noted that after classes of cryptography, interest in computer science among schoolchildren grew noticeably. If before the experiment students increasingly associated the concept "computer" only with programming and entertainment, after classes of cryptography, computer technologies were also associated with solving technological problems and puzzles, researching physical phenomena. This led to the conclusion that the goal of the course – attracting students to computer science – was generally achieved. In the future, German colleagues plan to add to the course the study of the Enigma cryptosystem and to develop advanced methodological manuals with online access for those who cannot attend full–time classes.

There is also a website ryptographiespielplatz in German [Krypt]. Their visitors can experiment with encryption and decryption of the most common symmetric ciphers: Vigenere and its modifications, encryption with the keyword and with the autokey. However, for schoolchildren it is less suitable because there is no theoretical basis for encryption.

In other cases, in Germany, cryptography training also takes place at the level of additional education and through inclusion in mathematics as one of the topics. In addition, for those who are fond of ciphers and cryptanalysis, the Spring School on symmetric cryptography is traditionally held in the city of Bochum. The "similar" situation is in Great Britain: a summer school for secondary and high schools is held in Dartmouth at the local university – the School of Mathematics at the University of Manchester. The Alan Turing Cryptography Competition is held to popularize cryptography among teenagers [DartN]; [ATCC].

3.3 The proposed method

We developed our own elective course on the fundamentals of cryptography for 7–9th–grade students, which is based on the experience of foreign colleagues. The course consists of the handbook on the elementary cryptography transformations. The elective course is based on the system–activity approach and elements of project teaching [Kuz18];[Smi18].

This course lasts for 36 hours. It was conducted for half a year in a group of 25 people at the Physics and Mathematics School of the city of Astrakhan (Russia). The classes lasted 1.5 astronomical hours and were held once a week.

The structure of the classes implied lectures and practical work. Control and independent works, as well as crossword puzzles and educational games where students could apply the acquired skills, were used to test the knowledge.

In addition, teaching software was developed for use the lessons of this course. The software allows improving the learning of basic cryptography transformations and the methods of encryption, based on them. The learning includes the introduction to theory and mathematics foundations of cryptography transformations (transposition, substitution, analytical transformations and gaming) using an example of a demonstration version of the current cryptosystems (Fig. 1).

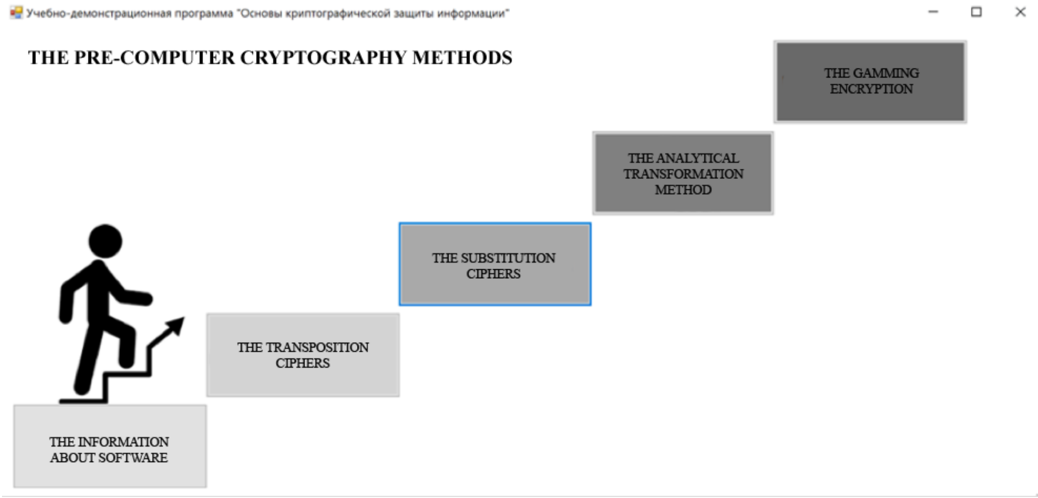

Figure 1: Software interface demonstrating four types of cryptographic transformations

The transposition ciphers are demonstrated on the example of “Double Transposition” and “Magic Squares” cryptoalgorithms. “The Wheatstone Double Square” and Vigenere cipher illustrates the substitution ciphers (Fig. 2). The gamming encryption is shown by the example of Vernam Cipher. Hill’s cryptosystem is used for the demonstration of the analytical transformation method. The software of the course also includes a module for testing and checking knowledge.

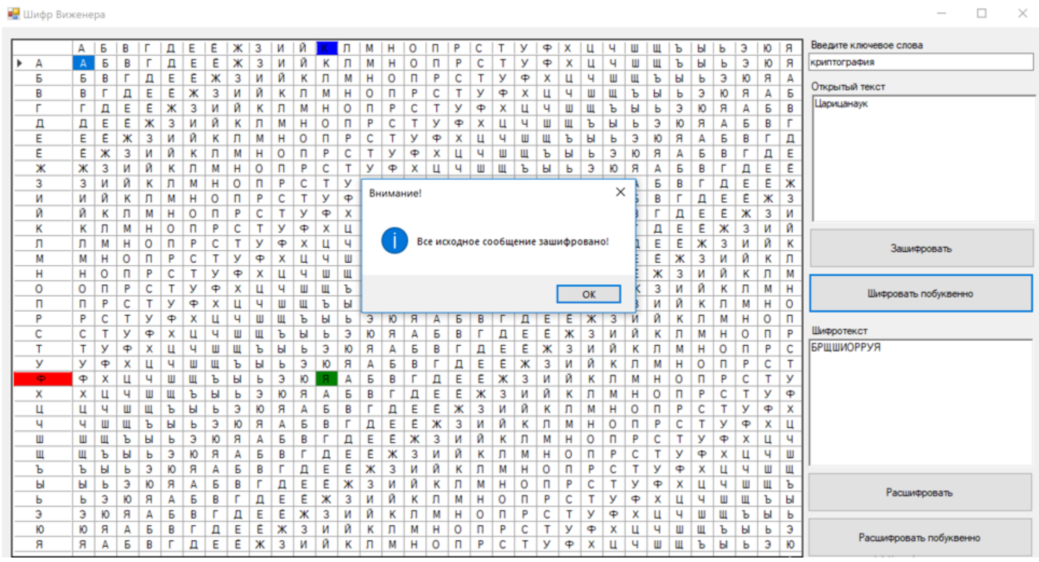

Figure 2: Software interface demonstrating the Vigenere cipher in letter–by–letter encryption mode

4 Results

Using the training course already provides an opportunity to evaluate intermediate results. Students who use this software as part of cryptography training are better at assimilating theoretical material. This is due to the fact, that students can visually study the process of cryptographic transformations, which are demonstrated in the program. This is marked by the results of control and independent work.

As for the level of development of systems thinking, tasks for input and output controls were developed for its measurement. With their help, the initial and final level of development of the system thinking of schoolchildren was determined.

Input control included the implementation of 20 tasks providing for the possibility of identifying various principles of systematization (finding an extra word in a row, anagrams–words, anagrams–sentences, and similar tasks).

In addition, during the input control, students were asked a question with a detailed answer: “Give an example of any system. Why do you think this is a system?” This question allows revealing whether the student in general understands “what the system is” at an intuitive level.

After passing the cryptography course students passed the output test with similar tasks on system thinking [Deu07]; [Syc09]. The result was evaluated on a five–point scale, where 1 – “very bad”, 5 – “excellent”.

The results in the Figure 3 below illustrate that the number of positive ratings on tests for system thinking (4 and 5) in the amount increased from 5 to 17, while the number of negative ratings (1 and 2) became significantly less, decreasing in total from 10 to 2.

According to student testing data obtained before and after the elective course, the following performance

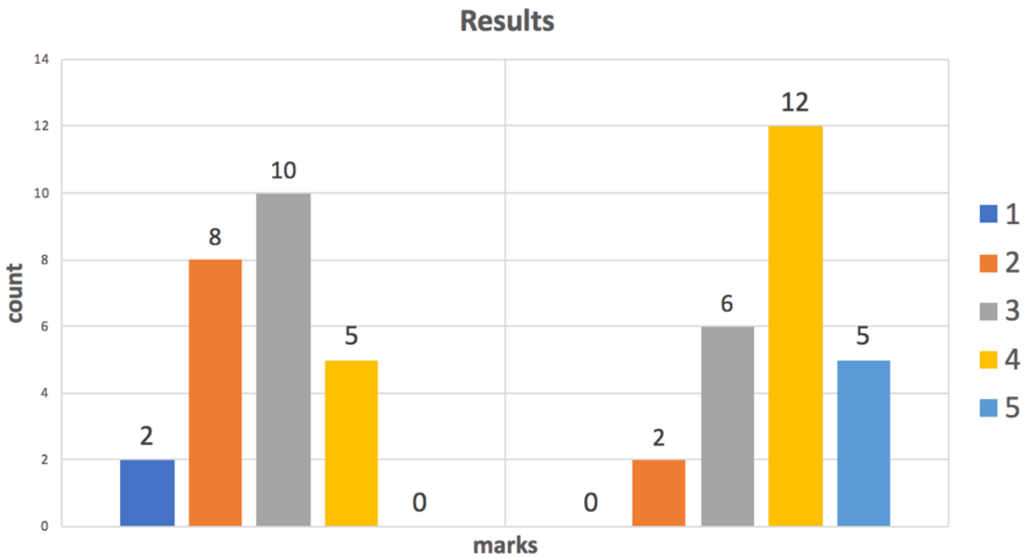

Figure 3: Comparison of focus group results in tests for system thinking on a five–point scale

indicators of the methodology were calculated from the point of view of the development of students' systemic thinking:

• K – the percentage of the quality of knowledge (the number of “good” and “excellent” grades from the total number of students' marks on the system thinking test);

• C – the percentage of academic performance (the number of positive assessments of the total number of students' marks on the system thinking test).

$$K = \frac{5+12}{25} - -\frac{0+5}{25} \cdot 100\% = 48\% \tag{1}$$

$$C = \frac{5+12+6}{25} - -\frac{0+5+10}{25} \cdot 100\% = 32\% \tag{2}$$

According to the results of input and output controls and calculations, it was noted that students after studying the course of cryptography showed an average of 40

Check optional course performance for systems thinking development was carried out with the help of statistical methods – calculating the distribution of the sum of squares of k–independent standard normal random variables using the X^2 criterion. The advantage of the method is that it allows comparing the distribution of signs presented on any scale.

For the null hypothesis H0, we accepted the hypothesis, when the two distributions do not differ from each other, in other words – the hypothesis that the students' systemic thinking did not develop in any way after studying cryptography. Hypothesis H1, on the contrary, says that the described statistical distributions are significantly different, that is, the results of the system–thinking test before and after the elective course indicate an improvement in students' systemic thinking.

To use the X^2 criterion, the results of input control of students were listed in the table 1 and presented in the form Q1i, where Q11 is the number of students with a rating of "1" and by analogy Q15 – students with a rating of "5". The output control results are processed in the same way and are listed in the table (Q2i). N means the number of students who participated in the input and output controls.

Table 1. Input and output control results

Results		**Input control**	**Output control**	**Amounts**
Ratings	"1"	$Q_{11} = 2$	$Q_{21} = 0$	$Q_{11} + Q_{21} = 2$
	"2"	$Q_{12} = 8$	$Q_{22} = 2$	$Q_{12} + Q_{22} = 10$
	"3"	$Q_{13} = 10$	$Q_{23} = 6$	$Q_{13} + Q_{23} = 16$
	"4"	$Q_{14} = 5$	$Q_{24} = 12$	$Q_{14} + Q_{24} = 17$
	"5"	$Q_{15} = 0$	$Q_{25} = 5$	$Q_{15} + Q_{25} = 5$
N		25	25	50

For hypothesis H1, the X^2 value is calculated using the following formula: Using the formula (1) and data

$$\chi_1^2 = \frac{1}{N_1 \cdot N_2} \cdot \sum \frac{(n_1 \cdot Q_{2i} - n_2 \cdot Q_{1i})^2}{Q_{1i} + Q_{2i}}$$

from the table 1, we perform the calculations:

$$\chi_1^2 = \frac{1}{25 \cdot 25} \cdot \left[\frac{(25 \cdot 0 - 25 \cdot 2)^2}{2} + \frac{(25 \cdot 2 - 25 \cdot 8)^2}{10} + \frac{(25 \cdot 6 - 25 \cdot 10)^2}{16} + \frac{(25 \cdot 12 - 25 \cdot 5)^2}{17} + \right.$$

$$\left. + \frac{(25 \cdot 5 - 25 \cdot 0)^2}{5} \right] = \frac{1}{25^2} \cdot (1250 + 2250 + 625 + 1801{,}47 + 3125) = 14{,}44$$

The critical value of 2 for the level of statistical significance p = 0.01 and df = 4 is 13.28. The resulting value is greater than the critical (14.44 ¿ 13.28). Therefore, the difference in the level of systemic thinking before and after the elective course is statistically significant and regular.

5 Discussion

After completing the elective course, a survey of students was conducted with the aim of sharing impressions and feedback on the classes held. 80% of the surveyed schoolchildren reported that after studying elementary cryptography, they began to think more often about information security issues in the context of their own life situations that they face daily when using personal or school computers. In addition, students began to pay attention to the fact that cryptography can provide not only confidentiality, but also other information security services (authenticity, non–repudiation), which indicates an improvement in their competence in this area.

References

[Vas04] I. P. Vasilego. *Teorija chisel v kriptografii (dlja shkol'nikov). Metodicheskie ukazanija.* (Number theory in cryptography (for schoolchildren): Methodical instructions). Orenburg, 2004. – Access mode: http://window.edu.ru/resource/085/19085, free. – In Russian, 2019/01/21.

[Bos 13] L. L. Bosova. Author workshop, 2013. – Access mode: http://lbz.ru/metodist/authors/informatika/3/, free. – In Russian, 2019/02/27.

[Dus17] R. V. Dushkin. *Shifry i kvesty. Tainstvennye istorii v logicheskih zagadkah*, 2011. (Ciphers and quests. Mysterious stories in logical puzzles). – Moscow: AST, 2017. – 288 p. – In Russian.

[Mat16] N. V. Matveeva. Author workshop, 2016. – Access mode: http://lbz.ru/metodist/authors/informatika/4/, free. – In Russian, 2019/02/27.

[Azi19] Web-portfolio of a teacher of computer science T. Yu. Azizova. – Access mode: http://tatiyanaasisova.narod.ru, free. – In Russian, 2019/02/27.

[Sem16] I.G. Semakin. Author workshop, 2016. – Access mode: http://lbz.ru/metodist/authors/informatika/2/, free. – In Russian, 2019/02/27.

[Tan05] E. V. Tanova. *Formirovanie kompetentnosti v oblasti zashhity informacii u shkol'nikov v processe obuchenija informatike*

(Formation of competence in the field of information security among schoolchildren in the process of teaching computer science): diss. cand. ped. sc. Chelyabinsk, 2005. – 173 p. – In Russian.

[Tan07] E. V. Tanova. *Vvedenie v kriptografiju: kak zashhitit' svoe pis'mo ot ljubopytnyh.*, 2015. – 921 with. (Introduction to cryptography: how to protect your letter from the curious). – Moscow: Binom, 2007. 80 p. – In Russian.

[Evl19] Site of a teacher of computer science A. V. Evlampyev. – Access mode: https://nsportal.ru/alexandr-0, free. – In Russian, 2019/02/22.

[ISOC] Interregional School Olympiad on Cryptography. – Access mode: http://v-olymp.ru/cryptolymp, free. – In Russian, 2019/02/21.

[Bei06] J. Beissinger, V. Pless. The project "Cryptography: The Mathematics of Secret Codes", Chicago, 2006. – Access mode: http://www.informalscience.org/cryptography-mathematics-secret-codes, free. – 2019/02/21.

[Sau08] B. Saunders, J. Beissinger. Using Cryptography to Teach Number Theory to Future Middle School Teachers // Paper presented at the annual meeting of the The Mathematical Association of America MathFest, TBA, Madison, Wisconsin, Jul 28, 2008.

[Bry17] L. Bryant. Caesar cipher: Introduction to cryptography. – Access mode: http://www.purdue.edu/discoverypark/gk12/downloads/Cryptography.pdf, free. 2018/11/21.

[Ber12] N. Bergner, J. Holz, U. Schroeder. Cryptography for Middle School Students in an Extracurricular Learning Place CSEDU 2012 - Proceedings of the 4th International Conference on Computer Supported Education, Volume 2, Porto, Portugal, 16-18 April, 2012. – Access mode: http://schuelerlabor.informatik.rwth-aachen.de/, personal read request. –2018/11/15.

[Krypt] Site "Kryptographiespielplatz". – Access mode: https://www.kryptographiespielplatz.de/index.php, free. – In German, 2019/02/28

[DartN] Dartmouth News. – Access mode: http://www.dartmouth.edu/ news/releases/2008/07/16.html, free. – 2018/02/21.

[ATCC] The Alan Turing Cryptography Competition. – Access mode: http://www.maths.manchester.ac.uk/cryptography_competition, free. – 2019/02/21.

[Kuz18] V. Yu. Kuznetsova. *Metodicheskie aspekty obuchenija simmetrichnym shifram v ramkah fakul'tativnogo kursa kriptografii dlja shkol'nikov* (Methodical aspects of training in symmetric ciphers as part of an optional course of cryptography for schoolchildren) // Collection of materials of VII International scientific-practical conference "Symmetries: theoretical and methodical aspects". Vol. 1. Astrakhan, 2018. Pp. 203-208. – In Russian.

[Smi18] M. O. Smirnova, V. Yu. Kuznetsova. *Proektnaja dejatel'nost' pri izuchenii kriptografii v srednej shkole (Project activities in the study of cryptography in secondary school) //* collection of materials of Russian scientific-practical conference "Project activities: a new look at education", april.24–25.2018. – Astrakhan: ASU, 2018. – Pp. 212-216. – In Russian.

[Deu07] D. V. Deulin *Razvitie sistemnosti myshlenija u detej 6-9 let v processe obuchenija* (The development of systematic thinking in 6-9 years children in the learning process): diss. cand. psych. sc. Moscow, 2007. – 122 p. – In Russian.

[Syc09] I.A. Sychev. *Pedagogicheskie uslovija formirovanija jelementov sistemnogo myshlenija uchashhihsja starshih klassov* (Pedagogical conditions of formation of elements of system thinking of students of senior classes): diss. cand. ped. sc., Barnaul, 2009. – 197 p. – In Russian.