Educational Technologies
Образователни технологии

RESULTS OF THE FIRST WEEK OF CYBERSECURITY IN ARKHANGELSK REGION

Olga Troitskaya, Olga Bezumova, Elena Lytkina,Tatyana Shirikova
Northern (Arctic) Federal University – Arkhangelsk (Russia)

Abstract. The question of the need to teach schoolchildren to use cyberspace safely is the most discussed today. The analysis of the methodological literature and Internet sources suggests that almost all the proposed materials are instructive in nature. Students are not involved in activity of cyber threat recognition and decision making in difficult situations. In addition, the proposed tools do not constitute ancomprehensive system that will allow schoolchildren to learn the basics of cybersecurity at school. This is led to holding the „The week of cybersecurity" event at school as a comprehensive means to prepare schoolchildren for safe behavior in cyberspace.The article describes the experience and results of the first week of cybersecurity in educational institutions of the Arkhangelsk region. This event made it possible to implement the proposed conceptual model of teaching the basics of cybersecurity at school.

Keywords: cybersecurity; schoolchildren; cyberthreat; a conceptual model; week of cybersecurity

1. Introduction

Today modern society faces the problem of safe use of cyberspace. It is especially relevant for residents of the Arkhangelsk region. This area is the largest subject of the Russian Federation in the European part of Russia, so it exceeds such European countries as France and Spain. Schoolchildren of the Arkhangelsk region strive to actively apply the opportunities of the global network in their daily lives. There are several reasons:territorial distance from the main cultural centers of the country, the need to use Internet resources in preparation for lessons, the desire to be in the center of events. However, the number of crimes committed with the help of the Internet against children is growing. This signals the need for purposeful formation of their behavioral skills to work safely on the Internet. Today there is a term for this global information space, consisting of many computers, devices that connect them, satellites, and allows you to organize communication through social networks, chats, telephone conversations. This is cyberspace. Laws and regulations apply in cyberspace and schoolchildrenshouldcomply them.So there is a special term "cybersecurity" for speaking of security in cyberspace. It includes a set of methods

and techniques designed to protect computers, computer networks, programs, and data from unauthorized access to, copying, alteration, or destruction of information.

The first Deputy Chairman of the Federation Council Committee on Constitutional Legislation and State Building L. N. Bokova stressed "Cybersecurity of children is a matter of state policy"[1] in March 2017. That is why in April of this year the parliamentary hearings "Actual issues of ensuring the safety and development of children in the information space" were held in the Federation Council. Methodical materials "Cybersecurity basics"[2] were presented there.These materials are recommendations for the dissemination and introduction of the course into educational programs of educational organizations. Its main goal is to give general ideas about security in the information society and then, on this basis, to form students' understanding of information security technologies and the ability to apply cybersecurity rules in all spheres of activity. In accordance with this goal, the authors identified eight modules of the course, for example, "Problems of Internet addiction", "Fraudulent activities on the Internet. Cybercrime", "Legal aspects of cyberspace protection", etc.For the organization of continuous training in the basics of cybersecurity, according to the developers, it is possible to supplement such school subjects as "Computer science", "The World around (natural Science)", "Fundamentals of life safety", with modules on "Cybersecurity basics" from 1 to grades.

The range of measures taken at the government level was supplemented by the order "On approval of the action plan for the implementation of the Concept of Children's Information Security for 2018-2020"[3]. This order was signed by the Ministry of Digital Development, Communications and Mass Media of the Russian Federation in February 2018. In accordance with this plan, it is planned to hold the all-Russian competition of social advertising on the topic of information security of children every year until December. Individual and collective works of children and adults, the works of legal entities are entitled to participate in it. In autumn 2018, it was held for the first time.Works for the competition could be presented in such nominations as „Video", „Video lesson", „Banner (poster)", „Information materials", „Websites and mass media about information security for children".

"Draft Guidelines for the implementation of measures aimed at ensuring the safety and development of children on the Internet"[4]has been developed for a number of categories of websites and services.This document contains a set of practical measures to protect minors from unwanted content, a list of functional buttons and links for equipment of websites and direct recommendations to owners and administrators of various websites on what they need to do in order to protect children.

Today there are a lot of Internet resources devoted to the formation schoolchildren' skills of safe work in the Internet. For example, the annual international Internet contest "Setevichok"[5] is held under the auspices of the Interim Commission of the Federation Council for the Development of the Information Society. Its goal is to teach children to learn successfully and safely using the Internet. Developed by Roskomnadzor specialists, the Personal Data portal[6] offers materials that allow children to understand the implica-

tions of using information technologies in their lives and provide decision-making tools in matters of virtual life.

The Fund "Reasonable Internet"[7] was established by the coordination center of the national domain of the Internet in 2012. The leading project of the Fund is the domain zone .ДЕТИ. It is addressed to children, their parents, teachers, organizations whose activities are aimed at training, development, social adaptation of children and adolescents. The developers indicate that this domain zone is designed to protect children from negative and dangerous information on the Internet. The peculiarity of children's perception is their absolute trust to the Internet information, contacts, communications, so special attention is paid to the threat of "negative" content. The authors claim that more than 40% of children in Russia are faced with images of a sexual nature on the Internet or other sources. And every sixth child of them sees sexual images every day or almost every day, every fifth child notes these images systematically 1 – 2 times a week. The problem of meeting online strangers remains one of the most important communication Internet risks in Russia. Half of Russian children constantly meet new people on the Internet, and 40% of children admit that they have met with Internet acquaintances in real life. That is why the domain zone .ДЕТИ, according to the creators, is a purely children's Internet space, collecting high-quality, interesting and safe entertainment content.

The website "Saving Children from Cybercrime"[8] is a means of developing schoolchildren' skills of safe work in the Internet. It is a public organization of the same name created on January 19, 2016 by parents of children who died as a result of cybercrime. The main purpose of the organization is to identify illegal actions against children on the Internet, to prevent crime, to organize assistance to injured children and their parents.There are articles on the issues under consideration, the laws that determine the responsibility of adults, instructions for parents and children: "Safe Internet", "Deadly impact on the child in social networks", "Rights, duties and responsibilities of parents".In addition, parents can watch documentaries, broadcasts, reports, interviews, telling about cybercrime and ways to deal with them, get acquainted with the process of setting up parental controls in the Windows operating system.

Despite the availability of information about the dangers of the Internet, it can be stated that all the proposed materials are instructive in nature. Children are not involved in cyberthreat recognition and decision making in difficult situations. In addition, the considered tools do not constitute an integral system that will allow children to learn the basics of cybersecurity in school. That is what led to the consideration of the need for the event "Cybersecurity week" in the schools as a comprehensive means to prepare children for safe behavior in cyberspace.

2. The week of cybersecurity as a form of implementation of the conceptual model of teaching the basics of cybersecurity at school

The European Convention on cybercrime identified the types of crimes. So, we took them as the basis of our conceptual model of teaching the basics of cyberse-

curity.We can talk about crimes against confidentiality, integrity and availability of computer data and systems, computer-related crimes (including computer fraud), about crimes related to child pornography, and about crimes related to violations of copyright.Accordingly, the purpose of teaching the basics of cybersecurity at school is to form children's understanding of the structure of cyberspace, the principles of work in it, the existing threats to Internet users, knowledge of the rules that will allow children to protect their personal data in the global network.

The goal can be achieved by solving the following tasks: 1) to introduce the basic concepts of cybersecurity, for example, through the use of instructions describing the rules of behavior in cyberspace; 2) to form pupils' ability to act in cyberspace through the application of a system of applied problems in computer science lessons; 3) to form pupils' behavior skills in situations of meeting with cyber threats through interactive games or using of simulators; 4) to create a cybersafe environment at home based on the educational materials offered to parents on parental meetings. We have defined the content of training in accordance with the identified types of cybercrimes, the goal and set objectives, taking into account the needs of the participants of the educational process and on the basis of the guidelines "Basics of Cybersecurity". The scheme of our proposed conceptual model for teaching the basics of cybersecurity is below (figure 1).

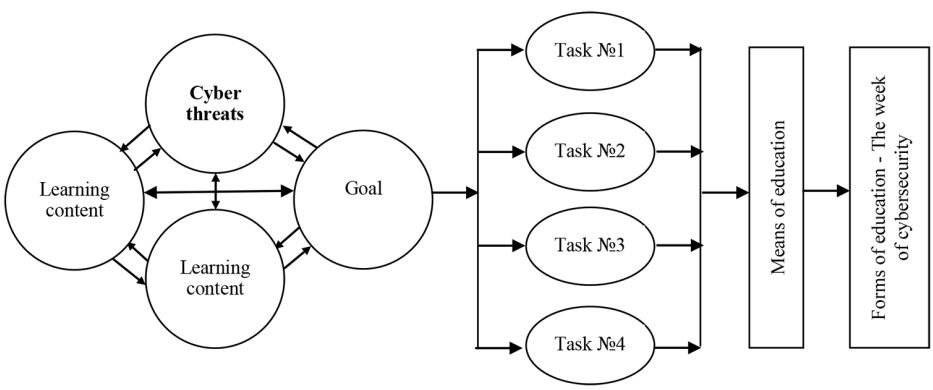

Figure 1. Conceptual model for teaching the basics of cybersecurity

In our opinion, the week of cybersecurity is one of the possible organizational forms to implement this model. In its framework, the following main activities are held: a classroom hour"Safe Internet", a competition for the best essay on the topic, revealing the features of cybersecurity, a drawing contest that allows to discover their creative potential and reflect their ideas about cyberspace, a contest of tasks on cybersecurity, parent meetings, the theme of which is "Cybersecurity".

The content of the classroom hour was determined by the methodical recommendations of the "Basics of Cybersecurity" and psychological and pedagogical features of children of the corresponding age period. For example, table 1 presents the distribution of the issues on cybersecurity for pupils of 5 and 6grades.

Table 1. Distribution of the issues on cybersecurity for pupils of 5 and 6grades

№	Modules of the course"Basics of Cybersecurity"	Topics for classroom hours (grade 5)	Topics for classroom hours (grade 6)
1	General information about PC and Internet security	What programs should be installed on the computer?	Threats to mobile devices
		Network games as mass entertainment. Freeandpaidgames	Who provides protection of cyberspace (Internet space)?
2	SafetyandEcology	Can a virus program break a computer?	First aid for problems in the Internet
		Harmful to health Information (psychological aspect)	
		Medical information on the Internet - is it always useful?	
3	The problems of Internet addiction	Types of dependence. How can I determine the presence of dependency	Types of dependence. How can I determine the presence of dependency
4	Methods to ensure the security of PC and the Internet. VirusesandAntiviruses	Search for information. How can you protect yourself from unwanted information?	What is antivirus protection? How can you treat a computer?
		Computer viruses: the goal of computer viruses and computer treatment	Protection of children in social networks
5	Fraud on the Internet. Cybercrime	Types of Internet fraud (letters, advertising, hunting for personal data, etc.))	The dangers of mobile communications. Suggestions for installing malicious applications. Fraudulent SMS
		Virtual friends - who are they?	
6	Netiquette. Psychology and network	Rules of communication on the Internet. Basicsofnetiquette	What is personal data? What information is "superfluous" about yourself and others on the Internet?
		The psychological impact of the Internet (aggression network, personal defense in network)	
7	Legal aspects of cyberspace protection		Property on the Internet. Copyright. Paidandfreeinformation

The classroom hour in the form of a popular science lecture with the use of interactive games allows schoolchildren to be interested, to draw their attention to the existing problems in cyberspace. Its structure is represented by two components. The first part is a twenty-minute interactive part, children include in the activities of acquaintance with new scientific materials. The schoolteacher as a lecturer asks a system of questions. He determines whether pupils have their own experience in operating with the concepts introduced.Next, he coordinates the pupils' everyday ideas about cyberspace and the threats in it with scientific knowledge. The construction of a new pupils' experience in the application of scientific knowledge will be continued in the second part of the classroom hour.

A didactic interactive game is included in the content of the classroom hour with the goal of involving schoolchildren in identifying Internet threats and making decisions in difficult situations. This game is composed in the format of the famous game "Own game" (Figure 2).

Figure 2. The start of the game "Security on the Internet" (Grade 6)

During the week of cybersecurity, schoolchildren were asked to write an essay on one of the possible topics: "Is the Internet dangerous?", "Social networks: good or evil?", "Cyberspace: a look from the inside", "Virtual personality – who is it?", "Cybercrimes: what should do not to become its victim?", "Internet addiction: causes and consequences". The pupil of the 9th grade of the school 36 of the city of Arkhangelsk, choosing the last topic, has highlighted not only the causes of Internet addiction, but also ways to deal with them.

So, he claims that those who love and want to communicate a lot are getting used to the Internet.These people have fear and difficulty getting to know other people for some reason. The virtual world replaces friends to them.That is why in order not to fall into this kind of dependence, the pupil suggests "to meet more often with friends and relatives outside the house, for example, in hikes, on holidays, to go in for sports together, to have a hobby" (figure 3).

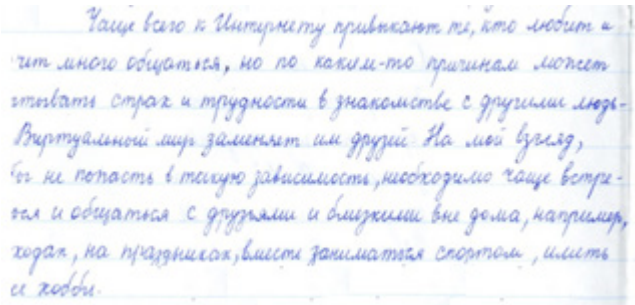
Чаще всего к Интернету привыкают те, кто любит и
чит много общаться, но по каким-то причинам может
тывать страх и трудности в знакомстве с другими люд-
Виртуальной мир заменяет им друзей. На мой взгляд,
бы не попасть в такую зависимость, необходимо чаще встре-
ться и общаться с друзьями и близкими вне дома, например,
ходя, на праздниках, вместе заниматься спортом, иметь
ие хобби.

Figure 3. Fragment of the pupil's essay (Grade 9)

A drawing competition was held as part of a week of cybersecurity. More than a thousand schoolchildren from the Arkhangelsk region from 5th to 9th grades took part in it. Children reflected ideas about cyberspace in their works. Their drawings make us think that cyberspace is fraught with many dangers. This form of the event made it possible to identify the goals of using cyberspace by children: communication in the network, assistance in preparing of homework, entertainment, for example, participation in on-line games or watching interesting films, animated films, buying necessary goods in online stores (figure 4).

Figure 4. Drawings of schoolchildren

During the week, meetings with parents of pupils were held in schools. The content of the parent meetings included the study of legislative acts in the field of cybersecurity, features of the application of anti-virus software and filter programs. It was obligatory to familiarize parents with cyber threats, especially with the so-

called “unusual” on-line games, existing “death groups”. The teachers described the behavioral characteristics of children who fell under the influence of such organizations.New knowledge has allowed parents to create an information-safe environment at home, to protect their children from cyber threats and to teach them to resist these phenomena of cyberspace.

The contest of tasks on cyber security was held at the Higher School of Information Technologies and Automated Systems of the Northern (Arctic) Federal University named after M. V. Lomonosov. This contest was the final event of week of cybersecurity. All contest’ tasks were compiled by students of the 4th and 5th courses of the training direction 44.03.05 Pedagogical education (profiles “Mathematics” and “Computer Science”) under the guidance of Associate Professors of the department of experimental mathematics and informatization of education. The material for contest’s tasks was selected on the basis of modules of the course “Cybersecurity basics” (Table 1).So, the contest of tasks on cybersecurity made it possible to determine the levels of readiness of schoolchildren to make informed decisions in situations of meeting with cyber threats.The tasks of the contest were applied in nature.The taskswere compiled taking into account the psychological and pedagogical features of pupils of different ages.Table 2 presents examples of tasks addressed to pupils in grade 5 in accordance with the four levels of readiness.

The official website[9)] was created for organizational and methodological support of the first week of cybersecurity. It was possible to apply for participation, get materials for events and get acquainted with the results of the contest of tasks on cybersecurity (figure 5).

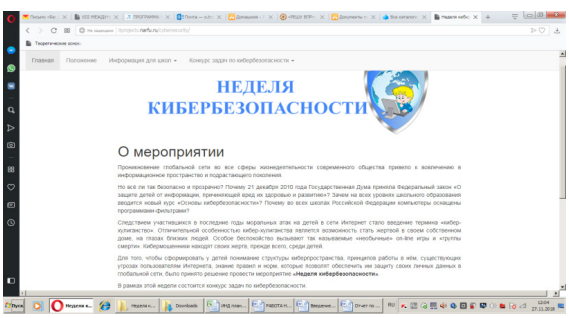

Figure 5. The main page of the website “The week of cybersecurity”

3. The results of the week of cybersecurity

The first week of cybersecurity was held from 22 to 27 October 2018. It was attended by pupils of 74 schools of Arkhangelsk, Severodvinsk and Arkhangelsk region, in particular Kholmogorsky, Shenkursky, Velsky, Kot-

Table 2. Levels of readiness to make informed decisions in situations of meeting with cyber threats

<table>
<tr><th>Levelsofreadiness</th><th>Feature</th><th>Typesofactions</th><th>Examplesoftasks</th></tr>
<tr><td>I</td><td>Level of representations about cyber threats and how to deal with them</td><td>Recognition, distinction, classification</td><td>Instructions: select a few of the correct answers from the proposed.
Task 1. The developer of the game “Stone” spent five years to create it.When “Stone” was released, the boy Misha really wanted to buy this game. Arriving at the store, he found that the cost of the game was high, so he decided to go to the Internet for help. Misha clicked on the first link in the browser and saw the inscription: “The game “Stoon” is free and you can download it from this link below”. From the options below, choose the one you would suggest to Misha.
a) Misha should download the game from this site, as it is free there.
b) Misha should ask his parents for money and buy the game in the store.
c) Misha should continue to look for the game on the Internet with the option to buy it at a discount.</td></tr>
<tr><td>II</td><td>Level of explicit knowledge about cyber threats and ways to deal with them</td><td>Reproduction, discussion, correlation, analysis</td><td>Instruction: establish the correspondence of the elements of two sets.
Task7.
<table>
<tr><th>Characteristic of Internet addiction</th><th>Types of Internet addiction</th></tr>
<tr><td>1. Permanent participation in online auctions</td><td>A. Game addiction</td></tr>
<tr><td>2. Obsessive fascination with computer games</td><td>B. Financial addiction</td></tr>
<tr><td>3. Constant participation in chats</td><td>C. Social addiction</td></tr>
</table></td></tr>
<tr><td>III</td><td>Level of skills and abilities in making decisionsat standard situations of meeting with cyber threats</td><td>Application of the acquired information in practice to a given class of phenomena and objects for solving problems requiring its literal application</td><td>Instruction: give a brief answer.
Task 13. Vasya was asked to make a report at the history lesson. Without thinking twice, he decided to find a ready-made version on the Internet.The boy entered the topic of the report in the search string and followed the first link. In the browser window he saw a bright button with the inscription “Download” and clicked on it. Suddenly, the computer started to reboot. Then he turned on, but all the shortcuts on the desktop disappeared. What happened to the computer? What actions should Vasya take to get out of this situation?</td></tr>
</table>

IV	Level of skills and abilities in making decisionsa-tunusual or unfamiliar situations of meeting with cyber threats	Application of the acquired information for the solution of the tasks demanding transfer of the gained knowledge in new conditions	**Instruction:** read the description of the situation and give detailed answers to the questions posed. **Task 16.**In one of the social networks the boy Igor met Vitya. After a few days of communication Vitya began to ask questions of a personal nature: “Where and with whom do you live?”, “Can you give me your phone number”, “Can you tell me about your family in more detail”, “Where do your parents work?”, “Do your parents earn a lot?” and so forth.Igor, without thinking about the consequences, told the interlocutor everything about himself and his family, and also sent family photos. After some time, Igor began to receive messages on the phone with the requirements of the transfer of money to the specified account.At the same time he was threatened that in case of non-compliance with the requirements, information about Igor’s relatives would be shared on the Internet. Make a list of mistakes that Igor made. How can you avoid the situation in which Igor found himself? Justify your answer. Make a recommendation for children who find themselves in a similar situation.

lassky, Pinezhsky, verkhnetoemsky, Kargopolsky, Krasnoborsky, Onega, Leshukonsky, Plesetsk and Primorsky districts. During the week, the teachers with the support of the school administration held classroom hour in grades 5 – 9, a cybersecurity essay contest, the drawing competition and parent meetings on the subject of “Cybersecurity”. A survey of parents of schoolchildren was conducted in one of the schools of Arkhangelsk. 290 people were interviewed. The results showed that most parents have acquired the necessary knowledge and skills in the field of cybersecurity. For example, 273 people know different types of cyber threats, previously – 65 (question 1). When answering the question of whether the model of behavior in situations of meeting with cyber threats was discussed with children, 281 people answered in the affirmative, previously-13 (question 2). The indicators for answering other questions have grown significantly: whether filter programs are installed on a home computer (question 3), whether children’s search engines are installed on a home computer (question 4), etc. The diagram with the results of two questionnaires on the example of questions 1 – 4 is shown in figure 6.

107 schoolchildren of grades 5 – 9 of Arkhangelsk took part in the contest of tasks on cybersecurity. This competition was held on October 27, 2018.The quantitative distribution of schoolchildren by the selected levels of readiness to make informed decisions in situations of meeting with cyber threats (by grades) is presented in table 3.

The primary analysis of the results shows that most schoolchildren recognize typical situations of risk, know the possible consequences of making the wrong decision, try to choose the most optimal strategy of behavior when meeting with cyber threats.

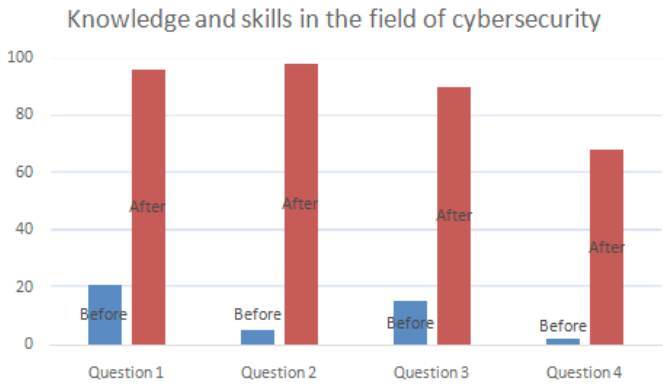

Figure 6 - The results of the survey of schoolchildren' parents

Table 3. Results of the analysis of the solution of tasks on cybersecurity in accordance with the levels of readiness

grade	Levels of readiness to make informed decisions in situations of meeting cyber threats			
	I	II	III	IV
5	1 pupil	3 pupils	4 pupils.	2 pupils
7	2 pupils	7 pupils	8 pupils	3 pupils
8	0 pupils	1 pupil	3 pupils	2 pupils
9	6 pupils	16 pupils	46 pupils	3 pupils

4. Concluding remarks

In the process of the study, it was established that all participants of the educational process should be competent in the field of cybersecurity. The best effect is achieved with a comprehensive approach to solving of this problem. We believe that it implies the annual holding of weeks of cybersecurity in educational institutions.In the future, the system of events of the week of cybersecurity should be complemented by a competition for independent compilation of cybersecurity tasks. It will allow more pupils to achieve the fourth level of readiness to make informed decisions in situations of meeting cyber threats. This competition will be held in two stages. The first stage is planned to be held in absentia. The best works will be selected on it. Their authors will be invited to the full-time stage. This stage will be held on the basis of the Higher School of Information Technologies and Automated Systems of the Northern (Arctic) Federal University named after M.V. Lomonosov.

NOTES

1. Council of Federation of the Federal Assembly of the Russian Federation. Official website(URL: http://council.gov.ru/events/news/78309/)
2. Methodical materials „Cybersecurity basics“ (URL: https://www.единыйурок.рф/osnovy)
3. Action plan for the implementation of the Concept of information security of children in 2018 – 2020(URL: https://digital.gov.ru/uploaded/files/2-proekt-plana-meropriyatii.pdf)
4. Draft Guidelines for the implementation of measures aimed at ensuring the safety and development of children on the Internet(URL: http://council.gov.ru/media/files/6evwqWEYBgoNPq6gP6SXdoP3smyHJABx.pdf)
5. Setevichok. V international quest for digital literacy. Official website(URL: http://www.сетевичок.рф)
6. About the project. Welcome to the children's page of the portal personal data! Official website(URL: http://персональныеданные.дети/o_proekte/)
7. The Fund „Reasonable Internet“. Official website(URL: http://интернет.дети/about/fond/)
8. Saving Children from Cybercrime. Official website(URL: http://62ru.ru/об-организации.html)
9. The week of cybersecurity (URL: http://itprojects.narfu.ru/cybersecurity/)

✉ **Dr. Olga Troitskaya, Assoc. Prof.**
M. V. Lomonosov Northern (Arctic) Federal University
17, Severnaya Dvina Emb.
163002 Arkhangelsk, Russia
E-mail: o.troitskaya@narfu.ru

✉ **Dr. Olga Bezumova, Assoc. Prof.**
M. V. Lomonosov Northern (Arctic) Federal University
17, Severnaya Dvina Emb.
163002 Arkhangelsk, Russia
E-mail: o.bezumova@narfu.ru

✉ **Dr. Elena Lytkina, Assoc. Prof.**
M. V. Lomonosov Northern (Arctic) Federal University
17, Severnaya Dvina Emb.
163002 Arkhangelsk, Russia
E-mail: e.lytkina@narfu.ru

✉ **Dr. Tatyana Shirikova, Assoc. Prof.**
M. V. Lomonosov Northern (Arctic) Federal University
17, Severnaya Dvina Emb.
163002 Arkhangelsk, Russia
E-mail: t.shirikova@narfu.ru