http://www.moderntechno.de/index.php/meit/article/view/meit25-02-048
DOI: 10.30890/2567-5273.2023-25-02-048

УДК [004.7-047.72]:656.2

METHODOLOGY FOR THE FORMATION OF COMPETENCES OF FIRST DEGREE HOLDERS IN THE DISCIPLINE «MATHEMATICAL FOUNDATION OF INFORMATION SECURITY»

МЕТОДИКА ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ У ЗДОБУВАЧІВ ПЕРШОГО СТУПЕНЯ З ДИСЦИПЛІНИ «МАТЕМАТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Pakhomova Victoria / Пахомова Вікторія
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Ukrainian State University of Science and Technology,
Ukraine, Dnipro, Lazaryan St., 2, 49010
Український державний університет науки і технологій,
Україна, Дніпро, вул. Лазаряна, 2, 49010

Abstract. *The proposed methodology "MathFISLearn" for the formation of competencies of applicants for the degree "bachelor" in distance learning in the discipline "Mathematical foundations of information security": 1) the study of basic mathematical concepts, theorems and methods in the following sections: the theory of divisibility; theory of decomposition; number theory; the theory of lichens and the theory of algebraic structures during lectures conducted using the "Zoom" system, 2) algorithmization and programming for the implementation of: Euclid's algorithm; extended Euclidean algorithm; Fermat algorithm; decomposition of the number by dividing by sampling; sieve of Eratosthenes; Miller's test and organization of relevant research during laboratory work, 3) acquisition of practical skills in solving systems of equations according to the module based on various mathematical approaches and means when performing independent work using recommended sources, 4) elaboration of theoretical material using lecturer presentations and passing testing in the "Lider" system.*

Keywords: *competence, distance learning, information security, mathematical concepts, theorems, tests, algorithms, approaches, tools.*

Introduction

Problem statement. The coronavirus and our "new life under fire" led to the use of distance learning, in particular in the discipline "Mathematical Foundations of Information Security" and the formation of relevant subject competencies among first-degree applicants under martial law, which confirms the relevance of the topic.

Analysis of recent research. Evaluation of competencies is the subject of research of such scientists as: Bykov V. Yu., Gurevich R. S., Gurzhiy A. M., Morse N. V., Ovcharuk O. V., Spirin O. M., Sysoeva S. O., Zhaldak M. I. and others. It is important to identify, analyze and summarize the experience of EU countries, significant international organizations and initiatives (UNESCO, ECDL, MICROSOFT, INTEL, etc.), as well as comparability for modern Ukrainian education in international studies of the quality of education (PISA, TIMSS, PEARLS) [1]. The analysis of recent research and publications revealed [1-7] the following: 1) the lack of unified information and communication technologies for training in the discipline "Mathematical Foundations of Information Security"; 2) lack of a general methodology for organizing information security using various mathematical methods and algorithms; 3) features of generation Z and the relevant features of training applicants for the first stage; 4) the need to use distance learning

under the condition of the current situation in the world, and became the basis for the development of its own methodology "MathFISLearn".

The purpose of the article is to develop a methodology for the formation of subject competencies among applicants for the degree of "bachelor" in distance learning in the discipline "Mathematical Foundations of Information Security".

1. Formation of subject competencies during lecture sessions

The proposed methodology "MathFISLearn" provides an opportunity for applicants for the first degree in distance learning in the discipline "Mathematical Foundations of Information Security" to study the basic concepts, theorems and methods in the following sections: the theory of divisibility; theory of decomposition; number theory; the theory of lichens and the theory of algebraic structures during lecture sessions (32 hours), After the lecture lessons, the applicant must work out theoretical material based on the compiled presentations of the teacher, which are located in the distance learning system "Lider" [3], and undergo appropriate self-testing. So, for example, when studying the theory of lichens, the applicant of the first stage must: 1) know the definition (modulo comparison and the basic properties of comparisons, the Euler function and its properties, the witness to the decomposition of the number, Carmichael number, etc.); 2) to proof theorems (lemma, Fermat's minor theorem, Fermat's theorem, Corcelt's theorem, etc.); 3) find solutions to problems based on the use of Fermat and Euler theorems.

Finding a solution to some practical problems in the discipline "Mathematical Foundations of Information Security" requires drawing up tables (Table 1 for calculating the largest common divisor).

Table 1. Using the advanced Euclidean algorithm (general view)

Remains	**Incomplete particles**	***x***	***y***
a	**–**	**1**	**0**
b	**–**	**0**	**1**
r_1	q_1	$x_{j-2} - q_j \cdot x_{j-1}$	$y_{j-2} - q_j \cdot y_{j-1}$
r_2	q_2	…	…
r_3	q_3	…	…
…	…	…	…
r_{n-1}	q_{n-1}	…	…

An example (Figure 1) shows the decomposition of the number 105/38 into a continuous fraction and the compilation of a table of subordinate fractions.

q_s		2	1	3	4	2
P_s	1	2	1*2+1=3	3*3+2=11	4*11+3=47	2*47+11=105
Q_s	0	1	1*1+0=1	3*1+1=4	4*4+1=17	2*17+4=38

Figure 1. Formation of subordinate fractions

2. Formation of subject competencies during laboratory work

The proposed "MathFISLearn" technique involves using guidelines [4, 5] the following laboratory works (16 hours): 1) fundamental division algorithms (Euclidean algorithm and extended Euclidean algorithm); 2) decomposition of the number into factors (by sampling and using the Fermat algorithm); 3) methods for generating prime numbers ("Eratosthenes' sieve" and the use of polynomial formulas); 4) lichen theory (linear comparison solution and Miller test), and also provides an opportunity for first-degree applicants to gain practical skills in algorithmization and programming. So, for example, from the theory of division, acquire practical skills in calculating the largest common divisor and the smallest common multiple based on: Euclid's algorithm; extended Euclidean algorithm; canonical decomposition of numbers, as well as compare the possibilities of different approaches based on the results of research conducted on the created programs.

3. Formation of competencies during the performance of independent work

The proposed method "MathFISLearn" provides an opportunity for applicants for the first degree when performing independent work on the basis of recommended sources [4, 6] to acquire practical skills in finding a solution to compare the first power by various mathematical means: Euler's theorem; properties of finite chain fractions; extended Euclidean algorithm; properties of comparisons by module. In addition, when performing independent work, the applicant can receive interesting information about the life and research of outstanding scientists, such as: Abel; Adamar; Bertrand; Carmichael; Corselt; Eratosthenes; Euler; Farm; Gauss; Germain; Goldbach; Leibnitsa; Maltsev; Mersen; Miller; Riman; Vinogradov and others, the contribution of which is studied in the framework of the discipline "Mathematical Foundations of Information Security".

4. The use of a research approach in distance learning

Boyko M. A., Hrynevych L. M. and Morse N. V. determine that "the research and cognitive method should become the most important component of the scientific program at all levels and in all branches of science" [2]. The directions of acquisition of research competence of applicants should include: analytical review of scientific sources; solving a system of comparisons by module based on the use of two approaches: according to the Chinese pastor theorem and by the substitution method; analysis of the results; formulation of conclusions.

Features of generation Z and the corresponding features of training applicants for the degree "bachelor" under modern conditions require the introduction of new methods [7] in the conditions of distance learning and the use of interactive teaching methods. So, for example, according to the "Teaching-learning" method, one applicant for the first degree, having created his own program, explains to another applicant and jointly conducts appropriate studies of numbers based on the use of various mathematical tools, in particular, according to Fermat's algorithm and the decomposition of a number by dividing by sampling, as well as a graphical interpretation of the Chinese remainder theorem.

Conclusions

1. The proposed methodology "LearnMathFIS" for the formation of competencies of applicants for the degree "bachelor" when studying remotely in the discipline "Mathematical Foundations of Information Security": the use of "Zoom" during lecture classes; performance of laboratory work on the basis of compiled programs; performing independent work using various mathematical methods and approaches based on recommended sources; conducting unit testing in the "Lider" system.

2. Based on the use of the proposed methodology "LearnMathFIS", the applicant for the degree "bachelor": firstly, masters the subject competencies in the discipline "Mathematical Foundations of Information Security"; secondly, it acquires practical skills in scientific activity in organizing and conducting research on the basis of the created programs and formulating relevant conclusions on the use of: mathematical apparatus; algorithmization; programming; organization of research and their results.

Literature:

1. Биков В. Ю., Овчарук О. В. Оцінювання інформаційно-комунікаційної компетентності учнів та педагогів в умовах євроінтеграційних процесів в освіті: посібник. Київ: Педагогічна думка, 2017. 160 с.

2. Гриневич Л. М., Морзе Н. В., Бойко М. А. Наукова освіта як основа формування інноваційної компетентності в умовах цифрової трансформації суспільства. Інформаційні технології і засоби навчання. 2020. т. 77. № 3. 1-26.

3. Дистанційний курс з навчальної дисципліни «Математичні основи інформаційної безпеки» для здобувачів ступеня «бакалавр» спеціальності «Кібербезпека»; укладач: доц. Пахомова В. М. Сертифікат ДК0304 від 03.07.2019.

4. Математичні основи криптографії: навч. посібник / Г. В. Кузнецов, В. В. Фомичов, С. О. Сушко, Л. Я. Фомичова. Дніпропетровськ: Національний гірничий університет, 2004. 391 с.

5. Пахомова В. М. Математичні методи захисту інформації. Методичні вказівки до виконання лабораторних робіт. Дніпропетровськ: вид-во Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна, 2010. 22 с.

6. Пахомова В. М. Математичні методи захисту інформації. Методичні вказівки до виконання курсового завдання. Дніпропетровськ: вид-во Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна, 2010. 11 с.

7. Khadim B. Mobile learning and education in the digital age. 2018. URL:

http://elearningindustry.com/mobile-learning-education-digital-age

Анотація. *Запропонована методика «MathFISLearn» щодо формування компетентностей здобувачів ступеня «бакалавр» при дистанційному навчанні з дисципліни «Математичні основи інформаційної безпеки»: 1) вивчення основних математичних понять, теорем та методів за наступними розділами: теорія подільності; теорія розкладання; теорія чисел; теорія лишків та теорія алгебраїчних структур під час лекційних занятій, що проводяться за допомогою системи «Zoom», 2) алгоритмізація та програмування щодо реалізації: алгоритму Евкліда; розширеного евклідового алгоритму; алгоритму Ферма; розкладання числа діленням методом проб; решета Ератосфена; тесту Міллера та організації відповідних досліджень під час лабораторних робіт, 3) придбання практичних навичків розв'язання систем порівнянь за модулем на основі різних математичних підходів та засобів під час виконання самостійної роботи з використанням рекомендованих джерел, 4) опрацьовування теоретичного матеріалу з використанням презентацій лектора та проходження тестування в системі «Лідер».*

Ключові слова: *компетентність, дистанційне навчання, інформаційна безпека, математичні поняття, теореми, тести, алгоритми, підходи, засоби.*