Development of Information Security Competency in Students

Davlatov Oybek Ganievich,

Abstract: This article describes methodological aspects of developing students' information security competencies. In the article, the author clarifies the essence of the concept of "information security", its various aspects, the relationship between the development of information security competency and information-analytical competence, as well as the methodological conditions of information-analytical function. In addition, he substantiates the importance of vitagenic education technology in the development of students' information-analytical competency, and, on the basis of experimental materials, the correlation between the components of development of students' information security competency.

Keywords: information, information attack, security, competence, competent, vitagenic, component

I. INTRODUCTION

The second half of the twentieth century is recognized as the era of development of rapid, wide-ranging information systems and telecommunication technologies, their penetration into almost every aspect of life and human activity, as well as the factor having influenced and influencing the globalization of information space and the development of the entire world. It is noteworthy that the need for active information exchange within the country and in the outside world is very high. Such rapid development of the information industry, the growth in its potential and its widespread use in various aspects of public and state life can be one of the most important factors determining the progress of humanity in the new 21st century.

In the modern world, special attention is paid to the protection of the younger generation from the influence of harmful information and to the development of their ideological immunity to fight against information attacks. In particular, the "Safe Internet" program has been developed in the USA, France, Germany and Russia, and an effective organizational and legal mechanism for the development of students' competencies in providing information security has been created.

Davlatov Oybek Ganievich, Uzbekistan State Institute of Arts and Culture, Doctor of Philosophy (PhD) in Pedagogical Sciences, Tashkent city, the Republic of Uzbekistan Phone: (+998 97) 7742032; e-mail: asil.2108@mail.ru

At the same time improving the technology of developing students' competencies in providing information security; improving the diagnostic and preventive system of students' self-defence against information attacks through national cultural heritage; explaining the pedagogical and psychological features of development of students' competencies in providing information security; identifying the methodological conditions of use of historical and cultural heritage; working out the technology for developing students' competencies in providing information security; improving the methodological system of development of students' competencies in providing information security are of great importance.

II. MATERIALS AND METHODS

Such methods were used in the research process as comparative-critical study and analysis of problematic political, philosophical, sociological, psychological and pedagogical literature, study of advanced pedagogical experience in higher education institutions, sociometric methods (questionnaire, interview, talk), pedagogical experiment, and mathematical and statistical analysis of results.

In the 2nd block of the curriculum (mathematics and natural sciences) of all higher education institutions, teaching the subject of "Computer Science and Information Technology" is planned. The course is aimed at studying the theme of "Information and network security and information protection", however, it does not address the issue of developing students' competencies in providing information security.

In general, as a result of the analysis of syllabuses for general-professional and specialty disciplines taught in the history direction of higher education institutions, the following conclusions were drawn:
- there are a number of subjects in the curriculum of bacherlor's degree courses that allow studying historical and cultural heritage: "History of Uzbekistan", "Archeology", "Methodology of teaching history", "History of culture", "History of arts", "Source studies", "Central Asian cities", "Museum management studies", "Auxiliary history", "Historical country studies", "History of Central Asian nations", etc.;
- there are also specialty and elective subjects aimed at developing students' competencies in providing information security: "Introduction of modern educational tools in teaching historical sciences", "Technology and design in teaching history", etc. However, the themes aimed at developing

Retrieval Number: B10610982S1019/2019©BEIESP
DOI:10.35940/ijrte.B1061.0982S1019

370

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

students' competencies in providing information security are not clearly reflected in the content of these subjects;

- in-depth study of the types of historical and cultural heritage depending on the object and subject of the course in the series of "History of Uzbekistan", firstly, allows students to master the rich heritage left by ancestors, and secondly, today when thinking about historical and cultural heritage objects in the context of intensive tourism development, students develop competence to have accurate information about them.

III. DISCUSSION AND ANALYSIS

Currently, the concepts of "information threat" and "information attack" are widely used in scientific consumption. If we focus on the etymology of these concepts, we can conclude that they can be used synonymously. In historical sources, the word "attack" is used more extensively. The term "attack" in its essence is also found in Great Amir Temur's book "Tuzuk-i Timuri". That is, in the chapters entitled "My fifth council in the days of attack", "My sixth council in the time of attack" and "My seventh council in the days of attack", the actions of the enemies and the measures taken against them are described. The great military leader, who always chose the path of enlightenment against ignorance, wrote: "I have counselled my enemies to be on my side with my sweet words and sweet stories, and extinguish the burning fire (rage) in their hearts with the water of the right action. That is how I wanted to entice them" [1; pp.24-28]. Thus, through such sources, it is possible to find out that the peace and tranquillity of the country was also attacked at that time and how they were handled.

An information attack or threat is a set of conditions and factors that threaten the vital interests of the individual, society and state in the information field.

According to experts, the complexity of coverage of the problem of information security is due to the fact that so far no commonly accepted comment has been made on this concept and it is explained in relation to the field of science. For this reason, it is necessary to determine the fact that the "security" does not exist without an object. As A.A. Streltsov rightly points out, the notion "security" is abstract "without a clear object", and it loses its essence" [2; p.12].

In sociological and psychological literature the use of the term "information and psychological security" has become a tradition.

Information and psychological security is an important effort aimed at the protection against the influence of accidental or deliberate information that could harm the state, society and the individual. According to experts, this is done for the purpose of: prevention of threats to the security of the individual, society and state in the information sphere; maintenance of confidentiality of information, prevention of its leakage, theft and loss in the mass media; prevention of distortion and falsification of information [3].

Thus, in today's globalized world, provision of information security is a key to preventing information damage. It is natural that in this process, along with the fight against evil deeds, the harm that can be inflicted on a variety of levels is prevented.

Students' information and analytical competence is the ability to apply their existing knowledge, skills and personal experience in the process of analytical-synthetic processing of information in a variety of types and forms in order to obtain new and qualitative knowledge.

Development of students' information and analytical competence requires a number of methodological conditions:

The first methodological condition is to teach students the technology of information and analytical activities. That is, it requires relying on levels of indirect, practical and independent research to determine the decision-making stages such as putting the problem, solution and implementation.

The second methodological condition is the introduction of differentiated practical tasks into the learning process, which require taking into account, analysing (differentiated cognitive method) and summarizing (integrated cognitive method) individual features in the perception of information.

The third methodological condition is the use of special information and analytical systems and software tools in the learning process.

Development of students' information and analytical competence, in turn, is related to personal information security and reflects students' readiness to deal with information threats from a personal value-orientated point of view characterized by the ability to perceive, analyse and evaluate information on the basis of existing experience.

Based on this definition, the following components of personal information security can be distinguished: cognitive (knowledge of the risks associated with the information environment, the ability to analyse and evaluate information), axiological (imagination of universal human values, and the ability to determine the behavioural models associated with these values), communicative activity (tolerance of others' opinions and points of view, the ability to assess the situation). The content of these components allows considering personal information security as a two-part structure: personal (system of personal traits, motivations and values) and activity-based (experience, knowledge, abilities).

The analysis of contemporary research allows identifying three approaches to addressing the problem of personal information security: the impact of the external environment, personal activity and integration.

The influence of the external environment is reflected in the restriction of access to harmful information and prohibition of its distribution by authorized persons. Evidence-based proof of the fact that students' copy information blindly through special programs and services can be an example of the prohibition on external influence. In fact, the older your age is, the less your chances of controlling information are, and moreover, you are constantly exposed to various information threats in your daily life. Unless you have a system of values that defines your attitude and behaviour,

you are vulnerable to information threats. It is well-known that in this process the goal cannot be achieved only by banning students, and this requires additional methods and means to provide personal security in the information environment. From this point of view, the activeness of a person is especially important in providing personal information security.

It is personal activeness that is of particular importance to student years with the increasing number of information threats at the expense of the expansion of social environment, sociability, need for cooperation, and search for a spouse and like-minded people. It is well known that students are mature as individuals, but only they are more exposed to information influences because of the expansion of their information space and mastering different ways of navigation in the information environment.

In this regard, providing students' personal information security requires an integrated approach that allows them to achieve an optimal balance between the environment and their individual capabilities. The environment is not secure to maintain personal security for a person with the inner strength and capabilities, and therefore, the person needs to be protected from threats. In this approach, it is the activeness of the individual that plays an important role in providing personal information security.

To develop students' competencies in providing information security, it is particularly effective to organize work on texts that require a hermeneutic approach. The technology of hermeneutic education and active and interactive methods (business games, trainings, discussions) create necessary conditions for students to properly evaluate the author's point of view and to further clarify their own ideas. Organization of students' work on texts is carried out in several stages: 1) motivational (creating motivation for receiving new information); 2) assessment (understanding and realizing the information, analysing the author's intentions); 3) communicative (problem-solving based on valuable approach); 4) reflexive (further refining the personal point of view). According to the contextual approach (A.A. Verbitsky) that draws students to a deeper analysis of reality, "content plays an important role" in understanding, that is perception of information [4; p.42]. In order to develop students' competence in providing information security, the texts selected should be systematized according to certain principles and meet the following requirements for the content: 1) presence of the threat of malicious information in the text; 2) existence of a problematic situation in the text to develop the ability to independently detect, evaluate and resist malicious information; 3) reflection of the real situation in relation to information threat; 4) formation of the axiological worldview in students.

IV. RESULT

Criteria, indicators and diagnostic methodologies were defined in accordance with the level of development of students' competencies in providing information security.

Flexible methodologies were used to determine the formation of axiological attitude to historical and cultural heritage, cultural and universal human values, as well as motivational and reflexive points of view. The author's methodologies were used to determine the formation of knowledge about information threats, knowledge to counter information threats, and basic competences to work with information on the Internet.

An analysis of the literature shows that similar approaches are used to determine the level of mastering activities. Only certain definitions and additions have been made in relation to own research.

In this regard, to determine the development of students' competencies in providing information security within the framework of the research, we have identified high (creative-value-oriented), medium (situational-reproductive) and low (slow-adaptive) levels according to the following score scales: high – 2, medium – 1, low – 0. Assessing each indicator in the form of scores determines the level of students' competence in providing information security. In order to determine the right level, significance grouping intervals have been established. For this purpose, A.A.Kyveryalga's methodology was used. According to this methodology, the medium level is determined with a 25% deviation from the medium in the assessment range in the form of score. In this case, the deviation indicators in low- and high-levels looks as follows: low level – from R (min) to $0.25 \ast R$; high level – from $0.75 \ast R$ to R (max), where R (min) denotes the lowest limit of score value, R (max) – the highest limit.

In the experiment, 440 students from Uzbekistan State Institute of Arts and Culture, Namangan State University, National University of Uzbekistan and Tashkent State Pedagogical University were involved.

The number of directions and respondents taken as the basis for the analysis of the results were as follows:

1) EG-1 – 32 students from Uzbekistan State Institute of Arts and Culture;
2) EG-2 - 30 students from Tashkent State Pedagogical University;
3) EG-3 – 33 students from Namangan State University;
4) CG – 33 students from the National University of Uzbekistan.

Students from one and the same university were selected to compare the results in EG-3 and CG (EG – experimental group; CG – control group).

The analysis of the results of the experiments held at the baseline stage by the criteria is summarized in Table 1:

Table 1: The level of development of students' competencies in providing information security (baseline stage)

Groups	Number of respondents	Level of mastering		
		Adaptive	Situational-reproductive	Creative
EG-1	32	56.25 %	21.88 %	21.88 %
EG-2	30	56.67 %	23.33 %	20.00 %
EG-3	33	54.55 %	24.24 %	21.21 %
CG	33	57.58 %	24.24 %	18.18 %

The results of the experiments at the baseline stage indicate the following levels of development of students' competencies in providing information security: adaptive (low) – 56%; situational-reproductive – 24%; creative – 20% (Table 2).

Table 2

Medium significance level of development of students' competencies in providing information security (substantive stage)

Average number of respondents	Level of mastering		
	Adaptive	Situational-reproductive	Creative
32	56 %	24 %	20 %

At the end of the formative experiments, the effectiveness of developing students' competencies in providing information security was re-examined and summarized in table form (Table 3).

Table 3

The level of development of students' competencies in providing information security (formative stage)

Groups	Number of respondents	Level of mastering		
		Adaptive	Situational-reproductive	Creative
EG-1	32	21.88 %	34.38 %	43.75 %
EG-2	30	26.67 %	40.00 %	33.33 %
EG-3	33	21.21 %	36.36 %	42.42 %
CG	33	51.52 %	24.24 %	21.21 %

The results of baseline and formative experiments indicate that the adaptive level of developing students' competencies in providing information security decreased by 2.36 times. On the contrary, it is possible to conclude that the situational-reproductive level increased by 1.53 times and the creative level – by 1.89 times.

The results of correlation analysis also show the fact that there were significant changes in all the components of students' competencies in providing information security (Table 4).

Table 4

Correlation results on the development of students' competencies in providing information security

Components	Medium mastering		Level of significance
	Baseline	Formative	
Cognitive	10.81	14.23	$p \leq 0.01$
Organizational activities	24.15	30.07	$p \leq 0.01$
Axiological	9.46	13.51	$p \leq 0.01$

V. CONCLUSION

Providing information security requires, first of all, analysing and evaluating information in a variety of information sources and identifying malicious information, as well as preparing students for the protection of themselves and members of society from the threat of malicious information and for the fight against it. It is necessary to create a system of informative-legal, software-technical, normative-methodological and socio-cultural competences for the development of students' competencies in providing information security as socially active citizens and future specialists.

Formation of students' information and analytical competencies, in turn, is related to personal information security. In this process, it is advisable to consider the unity and interrelationship between the components of cognitive (having knowledge of the risks coming from information environment, the ability to analyse and evaluate information), axiological (imagination of universal human values, and the ability to determine the behavioural models associated with these values) and communicative (being tolerant of others' opinions and points of view, the ability to assess the situation) activities

REFERENCES

1. Temur tuzuklari. / Translated from Persian by A.Saguni and H.Karomatov. – Tashkent: Publishing House of Literature and Art named after G.Gulam, 1996. – 34 p.
2. Streltsov A.A. The content of the concept of "provision of information security" // Information Society. – 2001. – No.4. – p.12.
3. Raimov Sh.U. Provision of information security is one of the most important areas of the national security strategy. / Current archive of the Academy of State and Social Construction under the President of the Republic of Uzbekistan, 2006.
4. Verbitsky A.A. Active learning in higher school: a contextual approach. – Moscow, Higher School. Publ., 1991. – 207 p. (in Russian).
5. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security: Vulnerabilities, Threats and Countermeasures. School of Multimedia, Hannam University, Daejeon, Korea. International Journal of Multimedia and Ubiquitous Engineering. Vol.3, No.3, July 2008.
6. Stamp Mark. Information security: principles and practice. USA, 2011. – 240 p.
7. Stavroulakis Peter, Stamp Mark. Handbook of Information and Communication Security. – 2010. – 178 p.