Olena MATVIICZUK-JUDINA[1]

Opiekun naukowy: Swietlana LOBODA[2]

KOMPETENCJE Z ZAKRESU GRAFIKI KOMPUTEROWEJ DLA STUDIÓW INŻYNIERSKICH, KIERUNKU: CYBERBEZPIECZEŃSTWO

Streszczenie: W artykule przedstawiono analizę współczesnych technik/metod nauczania grafiki komputerowej inżynierów na kierunku cyberbezpieczeństwo. Autor zaprezentował listę kompetencji, które powinny być uzyskiwane biorąc pod uwagę podstawowe dyscypliny akademickie.

Słowa kluczowe: elektroniczne zasoby w edukacji, przyszły specjalista informatyk, jakość edukacji, grafika komputerowa

COMPETENCE IN COMPUTER GRAPHICS OF BACHELORS OF CYBERSECURITY

Summary: The article covers the analysis of modern teaching techniques of computer graphics for bachelors of cybersecurity. The author presents a list of competencies that should be formed on the grounds of fundamental academic disciplines.

Keywords: electronic educational resources of education, future specialists of information technology, quality of education, computer graphics

1. Introduction

In domestic recommendations, the representation of competencies is that the basis of the interpretation of concepts is based on a common system of definitions, such as phrases: "ability to perform", "provide", "ability or capacity to demonstrate", "understand the theory and terminology", " understand and use effectively "," be capable ", and so on. There are various forms of coverage of competencies both in the domestic and in the world standardization system. For the formation of professional skills in computer graphics, the author presents a list of competencies that should be

[1] National Aviation University, Instytut komputerowych i informacyjnych technologii, Katedra komputerowych technologii multimedialnych, email: metalen3@ukr.net
[2] Prof., National Aviation University

formed on the grounds of fundamental academic subjects in higher education institutions (HEI). A new approach is proposed for the formation of competencies in infographics, holography, steganography of cybersecurity specialists.

1.1. Problem statement

Modern methods of implementation of educational and professional training of bachelors of cyber security in conditions of external aggression in Ukraine encourage the development of educational and practical data for the development of competences of bachelors of cybersecurity in the study of discipline "Computer Graphics".

1.2. The aim of the study is to

Identify the main factors for providing the skills and competences in order to form the infographic, holographic, and steganographic competent approach of bachelors of cybersecurity regarding the subject "Computer Graphics" (CG), develop and implement a methodology for providing initial practical knowledge, skills and abilities to form the competences for the theory of infographics, holography and steganography for the students acquiring the bachelor of cybersecurity in CG.

2. The content of infographics, holographic and steganographic competency training of computer graphics bachelors of cybersecurity.

Computer graphics as a component of professional competencies mostly refers to two modern properties of the information system, taking into account the world standardization system for the following classes:
- the protection of information resources and databases;
- the coverage of information flows of data.

Data protection includes the holographic protection of information resources and the infographics of various classes includes the coverage of information or data.

Exploring the system of international standards it should be noted that there is an urgent need to introduce additional lectures, practical materials, as well as laboratory complexes for the formation of knowledge of specialists studying the subject "computer graphics" in specialty 125 "Cybersecurity".

As an example the author suggests to consider the developed laboratory practices for the formation of competencies for bachelors of cybersecurity under the new method:
- the ability to provide holographic protection of information resources ICS (holography)
- the ability to design, provide and support various classes and types of infographic systems

Existing methods that solve the problem of copyright protection by embedding a sign-identifier, can be divided into two directions: the scientific and practical direction of the implementation of methods that conceal information in the digital aspects of the image; methods that embed a sign-identifier into a frequency domain with a tabulated or spatial reflection of a sign.

The first holographic method is the embedding of useful information directly into the digital plane of the image data based on 2D and 3D graphics, that makes them

unstable to unauthorized interference and various classes of distortion. Compression with loss, that violates the integrity of the sign, leads to partial, or even complete, destruction of the embedded identifier. Depending on various types of destruction, removal and compression procedures, there are methods that apply the reflection of the waves of the frequency range corresponding to the perception of the human eye. The basic limitation and the requirement of implementation of a sign-identifier is the integrity of the holographic system, built-in useful information with high probability of further distortions of integrity, or compression of the container image. The laboratory studies are performed on the applied software and graphic editors to implement embedding of graphic identifiers: Photoshop, FastStone Photo Resister, Avidemux, Watermark Magic, Image Tuner, etc. The work should be performed on the modern software applications of Photoshop CS5 \ 6 in order to implement the basic methods and means of holographic information protection using the features of compressors and file formats such as jpg, png, rar, etc.

A specialist in cybersecurity has to possess the knowledge, skills and abilities of the information security industry with the purpose of qualitative and most professional coverage of information and data technology infographics.

Infographics is not only the coverage of a large amount of information, but also the demonstration of the dynamics of object indication.

The work with infographics is always individual and professional and involves the search of optimal and minimized content of information.

The development of the infographics project with the purpose of forming professional competencies in cybersecurity education will provide the opportunity to professionally highlight the industry orientation on the basis of infographic technology.

The author offers thework based on Photoshop software application for the construction of the infographic object, illustrated by the Law of Ukraine on Cybersecurity. The specified infographics project contains subjects and objects of cyber defense, and so on. In order to specify the objectives and themes of the Law, the dark background and technology of overlay layers is used on the contrast to different text fonts, and methods of symmetrical objects are used to cause the psycho-emotional impact on the user. The project can be attributed to a class of work based on analytical research - analytical infographics.

A new approach to the formation of competencies of IT specialists and their safety is suggested through the system of international standards, world models of industry, and also based on the grounds of the basic properties of information systems, including:

- the protection of system information resources;
- the coverage of information and data.

The educational sections and lectures that directly deal with the protection of information resources and data for computer graphics can include following topics:

- steganography (the process of concealing critical video data);
- compression of the informational video stream;
- holographic protection of information resources;
- different classes and types of advertising activities of enterprises, organizations of various forms of ownership;
- infographic of different classes, etc.

The detailing of the formation of approaches and the list of competencies of specialists in cybersecurity on the subject "Computer Graphics" are presented in the author's studies.

Based on the above mentioned studies, corrections were made to the curriculum and a new list of professional competencies for the preparation of bachelors of cybersecurity was proposed in accordance with the developed methodology for the competencies formation in the subject "Computer Graphics".

As an example, the author proposes to consider the developed examples of laboratory work for the development of competencies under the new model for the formation of special competencies of specialists of the bachelor qualification level:

- the ability to provide a concealment of critical video information in ICS (steganography);
- the ability to provide holographic protection of information resources ICS (holography);
- the ability to design, provide and support various classes and types of infographic systems.

The competence in steganography is the ability to provide a process of concealing of information in a graphic message in the ICS.

Steganography is a secret record (from Greek: steganos - secret, secret; graphy - record). Steganographic technologies and methods of cyber protection of informational (useful) messages can be realized with the help of different systems and their properties, such as technical, physical, etc.

Hiding the useful message by steganography methods greatly reduces the likelihood or even makes it impossible to identify the fact of transferring of information. Steganography is a science that studies the ways and means of confidential messages concealing.

A steganographic container is a graphic message in which hidden information or confidential data (open text) will be placed (hidden). Any file or data stream may become a digital container if the container does not comprise useful informational message and it is called empty. A container with useful data is called a filled steganogram or steganocontainer.

Digital methods of steganography are used to hide the data properties of an information container are:

- A container file that does not require absolute accuracy of high-quality data processing can be changed with loss of quality or size, but without loss of the functionality of the file itself;
- Lack of special tools or inability of the human sensory organs to reliably distinguish the minor changes in file containers, that are the result of embedding a useful message.

The methods are distinguished by the types of containers that use text, audio, graphical or video media. Each dedicated class is aimed at maximizing the use of peculiarities of the area and its features. For example, graphic methods use features of human vision, such as sensitivity to contrast, size, shape, color, location, or overall quality of a digital image.

The way of embedding information (in a container) defines the division of methods into format and non-format.

Format are based on the peculiarities of the data storage format, which is a container file. As such, the format of storing an empty container is analyzed to find

those service fields in the file header, the change of which in the specific conditions will not affect the functionality of the container. These can be service fields that are not used by modern programs, not fully filled fields of comments, etc.

Non-format ones are based on embedding information directly into the data of a blank container file. These non-format methods are also divided into two classes of procedures of different types.

Currently, there are several commonly used approaches to conceal a useful informative message or open source text in a container file:

- direct embedding of an open text (image, text, data, etc.) into a container file;
- non-direct concealing of the open text, that is, the implementation of a step-by-step process of previous procedures of the open text transformation by the established algorithm or function (text, image or data encoding).

The data compression is a process of transforming data in accordance with established rules, algorithms, or functions that is performed in order to reduce the amount of information (file size). Compression is lossless (when it is possible to restore raw data without distortion), or with loss (recovery is possible with minor distortions or with controlled losses). Lossless compression is used when processing and storing of the software and critical data. Compression with loss is commonly used to reduce audio, photo, and video content. It is clear that steganography uses only the methods of compression without loss of information, taking into account the reproduction of a complete identical copy of the built-in open text.

The compression operations can be performed, for example, using an application for archiving data without loss of information such as the PKZI type of the company PkWare or another type of WinZip software (Corel file archivers and compressors). By data archiving, we will understand the compression process of data presented as image or text (useful information message). Of course, different data classes, especially, an informational message in the form of a contrasting, artificial or monochrome image, can be compressed with different types of archivers with varying degrees of compression and quality. However, in the suggested examples, we will recommend the use of an optimal archiver for both text and image.

In order to hide the compressed images of objects from the archive in the chosen graphic file, we will use software applications, and also specify the direct ways of finding the files:

- the encoded open text pict.zip (with encryption or not);
- the file container;
- the place of the further arrangement of a filled-in filole container with steganogram or steganocontainer secret_file.jpg.

In the future, it is necessary to perform reverse procedures for the removal of encoded open text and decompression of a graphic message. A steganographic file container should not differ from the expert's point of view, and subsequently the removed public logos should not be distorted.

An additional example of embedding an informational message may be the use of software to hide textual information in a PNG file or other types of formats.

3. Conclusions

The basic factors of formation of initial practical knowledge, skills and abilities for the purpose of formation of infographic, holographic and steganographic competencies for the bachelor of cybersecurity students are defined and determined.

REFERENCE

1. SMICIKLAS M.: The power of infographics. Indianapolis, Ind.: Que Pub. 2012.
2. MATVIICHUK-YUDINA O.: Key competencies of specialty "Cyber Security" of the subject "Computer Graphics" according to the industrial model of production. Zhytomyr National University, 4(2017), 93 – 98.
3. MATVIICHUK-YUDINA O.: Formation of competency in steganography for bachelors of specialty "cybersecurity" in the "computer graphics" discipline. National Pedagogical University. Kyiv CXXXV(2017)135, 262 – 266.
4. KONAHOVICH G.: Computer steganography processing and analysis of multimedia data. Educational Literature Center, Kyiv 2018.