Model of Informational and Cyber Security Synthetic Learning Environment Step-by-Step Implementation

Ivan Chychkan[1], Svitlana Spasiteleva[2], Svitlana Shevchenko[2], Yuliia Zhdanova[2], and Halyna Shevchenko[3]

[1] *Taras Shevchenko National University of Kyiv,64 Volodymyrska str., Kyiv, 01601, Ukraine*
[2] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[3] *Department of Economic-Mathematical Modeling and Informational Technologies, 2 Seminars str., Ostroh, Index, 35800, Ukraine*

Abstract

The paper is devoted to the creation and improvement of the informational and cyber security learning environment for using the latest informational technologies and innovative teaching methods. The issues of informational and cyber security education in Ukraine are considered. The requirements to the modern educational environment of the higher education institution are determined. The stages of step-by-step improvement of the traditional closed learning environment with the use of the learning management system to the network learning environment with the possibilities of further step-by-step virtualization and transition to the cloud are offered. The importance and expediency of creating a synthetic online learning environment with extensive use of open educational resources (cloud and mobile) to increase the competence of students in the field of informational and cyber security has been confirmed. The article considers the forms of organization of the educational process, modern methods, tools and teaching aids for the synthetic educational environment of higher education. Taking into account the results of research in the psychological and pedagogical literature and their own experience, the amount of theoretical and practical knowledge for the formation of students' specialized knowledge and skills to protect informational in cyberspace was defined. The comparative analysis of resources of open informational and educational space is carried out, selection criteria are defined and the technique of their use is offered. A model of continuous step-by-step improvement of the network learning environment with a gradual transition to an open, personalized, virtual, cloud-oriented, synthetic learning environment with a distance form of learning is proposed. It is proved that innovative educational technologies, open informational and educational resources, cloud and mobile services related to data protection, allow to train labour market in-demand specialists with practical skills of informational protection. The practical implementation of the proposed method was carried out on the basis of Taras Shevchenko National University of Kyiv and Borys Grinchenko University of Kyiv.

Keywords

Informational security, cyber security, synthetic learning environment, virtualization, open informational and educational space.

1. Introduction

A sign of the modern informational society is the growing influence of informational and communication technologies (ICT) on all spheres of human activity. Digital transformation becomes the basis of society, business, government. In the digital economy, human capital and informational technology play a crucial role in ensuring the sustainable development of society. “There is a need to

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: chychkan@fit.knu.ua (I. Chychkan); s.spasitielieva@kubg.edu.ua (S. Spasiteleva); s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); halyna.shevchenko@oa.edu.ua (H. Shevchenko)
ORCID: 0000-0002-0854-389X (I. Chychkan); 0000-0003-4993-6355 (S. Spasiteleva); 0000-0002-9277-4972 (S. Shevchenko); 0000-0002-9736-8623 (Y. Zhdanova); 0000-0002-8717-4358 (H. Shevchenko)

ensure the readiness of society for such processes, mastering key combinations of knowledge, skills, thinking, attitudes, and other personal qualities in the field of informational and communication and digital technologies (digital competence)" - emphasizes the Concept of digital competences approved March 3, 2021 № 167-r [1]. Digital competence is understood as a dynamic combination of knowledge, skills, abilities, ways of thinking, views, other personal qualities in the field of informational and communication and digital technologies, which determines a person's ability to successfully socialize, conduct professional and / or further educational activities using such technologies [1]. In this regard, and taking into account the needs of the market and current trends the training of highly qualified specialists in digital technology is of particular importance. To maximize the potential of digital technologies new professionals with modern knowledge, digital skills, capable of self-learning, solving complex problems in a constantly changing environment are needed [2].

Significant work has been done by the European Community to build capacity for the digital transformation of education, in particular to change the skills and competence requirements of citizens. The work focused on developing a framework for digital competence for citizens (DigComp), educators (DigCompEdu), educational organizations (DigCompOrg) and consumers (DigCompConsumers). Much attention is paid by international and European institutions to the development of digital competence standards.

The latest informational technologies not only produce new opportunities, but also create new and unfamiliar risks of cyber threats, which can prevent companies and government agencies from realizing their digital potential. One of the components of digital competence is informational security: protection of devices, personal data and confidentiality. Digitalization should be accompanied by an increase in the level of trust and security, "raising public awareness of the dangers of the Internet" [1].

The formation, development and implementation of a national culture of cybersecurity are necessary in the fight against cybercrime. At the same time, there is a need to form basic knowledge of informational and cybersecurity for future professionals in almost all areas of training. The highlighted problems give a convincing idea of this study relevance.

2. Development of Cyber Education in Ukraine

Informational protection issues have long been one of the first tasks to be solved in the process of using modern informational and communication systems. Recently, the real losses from unauthorized access to corporate informational continue to grow. According to experts, internal leaks of corporate informational have more negative consequences than external interventions. In 2020, companies lost 3 times more corporate data through the fault of their own employees than as a result of hacker attacks, with 64.5% of accidental data leaks caused by the company's employees [3]. Most threats to the integrity and confidentiality of informational circulating in computer systems can be prevented through the use of methods and means of protection in the appropriate training of employees. Law of Ukraine of 05.11.2017 #2163-VIII "On the basic principles of cybersecurity of Ukraine" defines the need to "increase digital literacy of citizens and the culture of safe behavior in cyberspace, comprehensive knowledge, skills and abilities necessary to support cybersecurity goals, implementation of state and public projects to raise public awareness of cyber threats and cyber defense…" [4]. The culture of safe behavior is aimed at ensuring the cybersecurity of the individual both in the business processes of the organization and in its daily life.

Informational and cyber security skills are an integral part of digital competence skills, as emphasized by domestic and foreign researchers. Diorditsa IV in its publications emphasizes the need to deploy special and general cyber education, which should become a National Cyber Education Strategy [5]. In the works of Buryachok VL, Bogush VM, Folding PM a model of training specialists in the field of informational and cyber security in higher education institutions of Ukraine is presented [6]. The authors' research [7] is devoted to the future specialists in economics and management safe basic behavior in cyberspace formation in the educational process. Analysis of publications on cyber education by such authors as G. Austin, A. Henry, M. Kaminska [8] G. Marshall, K. Daimi, D. Thornton, S. Knight [9], O. Burov [10] showed that a single system, methodology and content of training on general cyber education has not yet been formed. All scientists emphasize that modern

educational technologies must be used for the specialists training (both technical and humanitarian) in informational and cyber security.

The article considers the model of an informational and cybersecurity synthetic learning environment step-by-step implementation and ways to implement it for the specialists in economics and management training in the courses "Informational Security," "Informational Security," "Cybersecurity" during 2017-2021 and specialists specialty 125 Cybersecurity during 2020-2021.

In the approved standards of higher education of Ukraine for the specialists training in the knowledge field 07 "Management and Administration" (specialists in accounting and taxation; finance, banking and insurance; management; marketing; entrepreneurship, trade and exchange activities) and the field knowledge field 05 "Social and behavioral sciences "specialty" Economics" defined such competencies as the ability to use specialized informational systems and computer techno"logy in relevant fields, the ability to use modern ICT to search, process and analyze business informational. The training of future specialists in economics and management should reflect the future directions of development of the working environment and ICT for the use of digital technologies in a single informational space – cyberspace.

Management and economic activities in accordance with the standards of higher education require professional knowledge of management, banking, entrepreneurship, trade, etc., as well as requires theoretical and practical knowledge of the use of interactive informational environment. Economics and management professionals must be able not only to receive and update informational, but also to process, store and create new informational in the global network environment. It is important to train specialists in economics and management to perform the task of informational protection, which involves the ability to use a set of special means of protection: legal, physical, engineering, cryptographic [11].

3. Requirements for the Synthetic Learning Environment

In the innovative development of higher education there is a constant improvement of the learning environment (LE) through the introduction of modern ICT and new teaching methods. LE training of specialists in economics and management in higher education institutions (HEI) should meet the requirements of the informational society and digital communication environment, encourage the search for approaches to formate future specialists in economics and knowledge management in cyberspace, determine the scope of this knowledge and search modern tools for acquiring such knowledge by creating a modern LE. Such an environment can be created with the use of an open informational and educational Internet space, a networked educational environment of free educational institutions, which will ensure cooperation of subjects of training, communication, storage of large amounts of educational material, planning of educational events, etc.

The problem of formation and development of computer-oriented educational environment in educational institutions was studied by domestic and foreign scientists, in particular V.Yu. Bikov [12], A.M. Gurzhiy, VV Lapinsky [13], SG Litvinova [14], O.Yu. Burov [15], Wilson S., Shafert S. and others. V. Yu. Bykov notes that to design an LE is "means to theoretically investigate the essential target and content-technological (methodological) aspects of the educational process to be carried out in an LE, and on this basis to describe the necessary composition and structure of an LE…" [12]. Analyzing the stages of formation of LE, we can note the constant growth of requirements in accordance with changes in the development of ICT. Mankind's transition to the informational age is accompanied by the emergence of new LE aspects, which are gaining rapid development and opportunities [14]. In the work of Pinchuk O. P., Lytvynova S. G., Burov O. Y. [15] features of development of network, virtual, mobile, personalized, cloud-oriented LE are considered. There is an increasing role of open computer-oriented LE with the use of computer teaching aids and electronic educational resources that are part of the ICT system of the educational institution, as well as tools, resources and services of open informational and communication networks. In [15] the synthetic learning environment is considered, the authors state that the synthetic learning environment is a step towards a new education. The prevalence of the term "synthetic learning environment" in the English literature is associated with the emergence and rapid development of e-learning tools that create new opportunities for education, development and new forms of human socialization. "Synthetic environment" is considered in two

aspects - artificial environment and synthetic as is formed due to the synthesis of the real physical world and the results of simulation and modeling [15]. Changes in the forms, methods and means of education are accompanied by changes in the organization of LE—direct communication mediated through the digital space, mixed, clouds, social networks, mobile technologies and more. In fact, human life is increasingly shifting to a synthetic environment, and activities, communication, learning, leisure are increasingly taking place in cyberspace with its advantages, disadvantages and dangers. The tendency to transfer educational and developmental activities to a synthetic environment is determined [16]. The purpose of the study is to theoretically substantiate and develop a method of step-by-step creation of a personalized, mobile, cloud-oriented, synthetic learning environment for the formation of informational security skills in cyberspace.

4. Development and Improvement of the Synthetic Learning Environment

In accordance with the purpose of the study, the following tasks are set:

1. Investigate the problem of using the network environment and modern ICT tools in the training of future economists and managers. Determine the purpose and objectives of the use of synthetic LE.
2. Determine the content of training: the amount of theoretical and practical knowledge for the formation of comprehensive knowledge, skills and abilities in informational security and informational protection in cyberspace in the training of specialists in economics and management.
3. Develop criteria and indicators for the selection of open educational resources on informational security and informational protection. Open learning resources include both server (cloud) and mobile resources.
4. Describe the method of using cloud-based emergencies: to determine the forms of organization, methods and teaching aids for the formation of knowledge, skills and abilities in informational and cyber security.
5. Identify ways to gradually virtualize the learning process and the transition to a synthetic LE.
6. Check the effectiveness of the use of LE to obtain knowledge of informational and cyber security of economics and management.

4.1. The purpose of using a Synthetic Learning Environment

The main trends of the modern education system are personalization of learning, adaptive learning, development of non-formal education, openness and accessibility of education, mobile learning. Learning is increasingly being transferred to cyberspace. Free educational institutions do not keep up with such a rapid development of ICT and modern teaching methods and tools. The EIA uses a closed LE with the use of a learning management system implemented on the basis of an open platform, for example, MOODLE. It is a structured multidimensional LE, which combines the possibilities of traditional learning with modern informational technologies based on the automation of teacher-student interaction [14]. Such an environment is limited in terms of the composition and structure of its components and therefore has limited didactic application. Given that at the Department of Informational Systems and Technologies of Taras Shevchenko National University of Kyiv and at the Department of Informational and Cyber Security named after Professor VL Buryachok. M. Hrinchenko Kyiv University traditionally uses closed LE situations using distance learning systems, there is a need to develop a methodology for creating a network LE with the possibility of further phased virtualization and transition to the cloud and create a synthetic learning environment. The practical implementation of this approach began with the creation of a network LE in the training of Economiks Faculty specialists (specialties of economics and management) in the training courses "Informational Security", "Informational Security", "Cybersecurity". The step-by-step transition to the creation of a cloud-oriented LE with the extensive use of open informational and educational space and innovative learning technologies will allow to adapt to the individual needs and capabilities of each student in acquiring the necessary professional competencies.

The purpose of forming a modern network LE in the study of disciplines "Informational Security", "Informational Security", "Cybersecurity" is to increase the level of complex students knowledge, skills and abilities in informational and cyber security formation in of all fields, including 05 and 07. LE in

informational and cyber security is the improvement of educational and methodological complex of the above disciplines. To obtain the necessary practical skills to protect informational in cyberspace, it is necessary to use a variety of educational resources, forms of the educational process organization, modern teaching methods and tools. The combination of different forms, methods and tools of teaching will help to achieve the desired level of learning material.

4.2. Formation of Informational and Cyber Security Skills

A modern specialist in economics and management in accordance with the standards of higher education must be able to work with informational, use modern ICT for the accumulation, processing, presentation of operational data and results analysis. Equally important is the acquisition of knowledge on the informational protection and the development of informational security strategies.

Obtaining comprehensive knowledge, skills and abilities in informational and cyber security is provided in the study of disciplines "Informational Security," "Informational Security," "Cyber Security," which are the variable part of the educational program to train specialists in relevant specialties in economics and management. In accordance with the approved work programs of the above disciplines, students must:

- Know the basic concepts and definitions of the basics of informational and cybersecurity
- Know the problems and main threats of informational and cybersecurity
- Know the basic technologies of network security, security rules for working with network services
- Organize work, public and domestic social space according to safety rules
- Set up a personal profile and communication tools in various online communities
- Know the principles of multilevel protection of corporate informational systems, technologies for detecting and preventing intrusions, informational security management
- Know the stages of designing informational security systems
- Be able to analyze informational flows and identify threats
- Be able to choose methods of informational protection and apply them in practice to protect informational from unauthorized access
- Plan and implement cybersecurity measures when creating digital content
- Organize the security of data and working informational systems when working with personal data and copyrighted content
- Assess the possible risks of placing personal data on Internet resources
- Design and use a secure informational environment for business organization

Classical forms of education with the study of the necessary theoretical principles, mathematical methods of informational transformation, construction of appropriate algorithms and programs and their study of various characteristics is unacceptable due to the limited number of hours and insufficient technical training of students. How to reduce the time of studying such topics without losing the quality of the future specialist - this is an interesting task faced by various free economic zones. This task requires an analysis of the possible use of existing open resources and the use of new forms and methods of teaching.

4.3. Criteria for Selecting open Educational Resources on Informational and Cybersecurity

According to a survey of university students on ways to improve the educational process [17], students determine the need to use different types of educational resources and the inclusion of open certified courses in the relevant disciplines. The opportunity to obtain practical knowledge and certificates from the world's leading educational institutions and companies motivates students to conduct independent research work and acquire a specialty in the field of informational and cyber security. Due to the transition to distance learning in quarantine, this opportunity is especially relevant. For example, the Faculty of Informational Technology and Management of the Borys Hrinchenko University of Kyiv offers free study of 4,262 Coursera University courses, developed by the world's

leading universities with a certificate (https://www.coursera.org/browse). In the table. 1 provides key informational on safety-related learning resources.

Table 1
Comparison of open resources on informational and cyber security

Resource name	Web address	Training courses	Language	Payment (+/-)	Description
Networking Academy CISCO	https://www.netacad.com/	Introduction to Cybersecurity Cybersecurity Essentials CCNA Cybersecurity Operations CCNA Security	English, Ukrainian	-	Requires teacher certification. The knowledge in the field of cybercrime, technologies for network protection. For entry-level network security professionals.
Microsoft Virtual Academy	https://docs.microsoft.com/en-us/ learn /modules/ security-in-m365/ https://docs.microsoft.com/en-us/learn /modules/ security-with-microsoft-365/	Introduction to security in Microsoft 365 (7 Units) Secure your organization with built-in, intelligent security from Microsoft 365 (6 Units)	English	-	Microsoft Security Management Solutions. Providing an integrated approach to security, data protection, applications and devices in the local, cloud and mobile network.
Coursera	https://www.coursera.org/browse/informational-technology /security	Introduction to Cybersecurity for Business Cybersecurity for Business Specialization IT Fundamentals for Cybersecurity Specialization	English	+/-	There are 41 courses for beginners from the world's leading universities and companies
Magnetic One Academy	https://magneticone.academy/course/informational-safe/	Basic course on informational security (10 topics, test tasks, supporting materials, examples and practical video lessons)	Ukrainian	+	To increase the level of informational security of the company, protection of infrastructure, intellectual property, confidentiality of informational. More than 150 practical recommendations for minimizing informational security risks.

Pro-metheus	https://edx.prometheus.org.ua/courses/KPI/IS101/2014_T1/about	Fundamentals of informational security	Ukrainian	-	Platform of open online courses. Basic rules for the use of personal informational in physical and virtual space. Electronic finance security rules.
Computer Security and Networks	https://www.coursera.org/learn/cyber-security-domain https://www.coursera.org/learn/usable-security	Cybersecurity and Its Ten Domains Usable Security	English	-	An open online course on cybersecurity and its components. Rules of joint communication and interaction on the Internet.
Using Future Learn	https://www.futurelearn.com/courses/introduction-to-cyber-security	Introduction to Cyber Security	English	-	Fundamentals of knowledge and skills in cybersecurity. Protection rules of digital life.

To justify the choice of open educational resources, the following selection criteria are defined:

• organizational (accessibility, ease of use, number of users, user roles);

• functional-didactic (course program, modularity, presentation of educational material in different formats, testing, magazine, calendar).

According to these criteria, free courses of the International Network Academy CISCO were chosen as the basic resource [18]. In Fig. 1 presents the available courses.

Figure 1: Cisco Networking Academy courses (https://www.netacad.com/portal/teaching)

Among the selected educational resources, the course "Cybersecurity Essentials" Networking Academy CISCO (see Fig. 2) is used as an element of the disciplines "Informational Security," "Informational Security," "Cyber Security." Microsoft Virtual Academy and other courses are offered to be used for independent work of students.

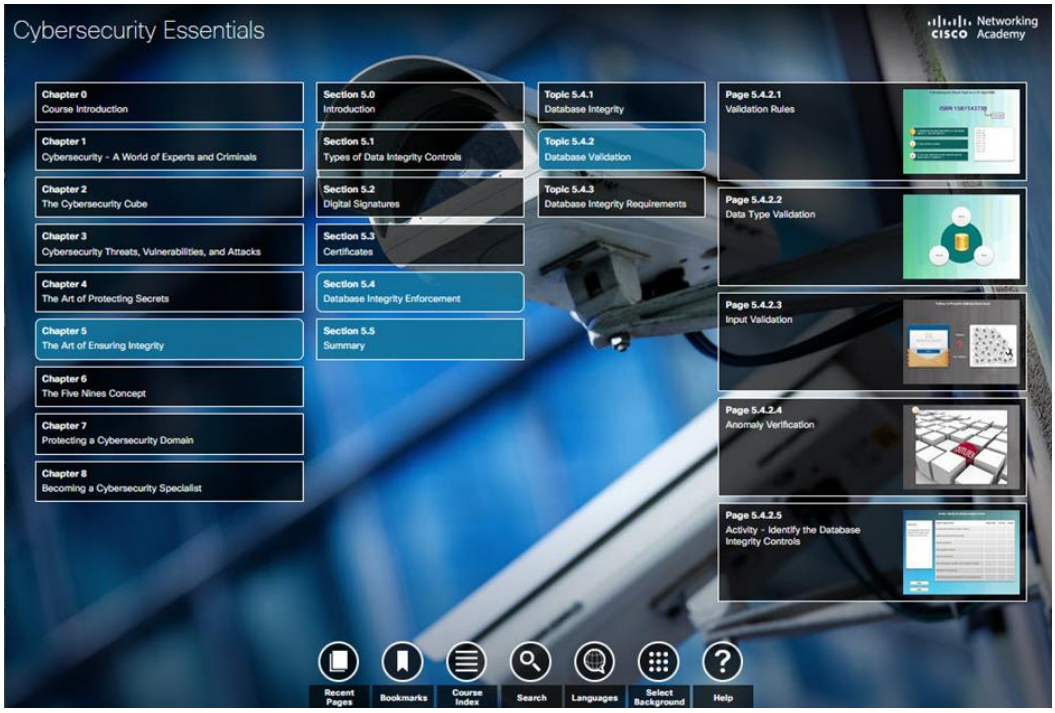

Figure 2: Course page «Cybersecurity Essentials» Cisco Networking Academy

4.4. Use of Mobile Applications for Informational and Cyber Security

Open learning resources include not only server (cloud) but also mobile resources that can be used to organize mobile learning for students. Students strive for convenience and mobility in the fields of teaching and research (writing articles, participating in conferences, developing scientific topics) [17]. Mobile technologies together with other informational and communication technologies, such as cloud data warehouses and cloud computing, can significantly increase the efficiency of students' independent work [19]. Mobile learning (M-Learning)—a modern direction of development of distance education systems using mobile phones, smartphones, tablets, PDAs [20]. Educational resources and informational can be stored in cloud storage and accessed from a variety of mobile devices, regardless of location and time. The power and capabilities of mobile devices are constantly growing, so they can be widely used as convenient and modern educational tools that contribute to the acquisition of new knowledge.

Mobile devices facilitate the understanding of educational material with the help of various subject mobile applications. Mobile augmented reality applications allow to build a visual model of educational material that develops the spatial imagination of students and provides an understanding of the processes, properties of educational objects [21]. Fig. 3 shows mobile applications related to cybersecurity. Antivirus programs, devices for protection of devices and applications are presented.

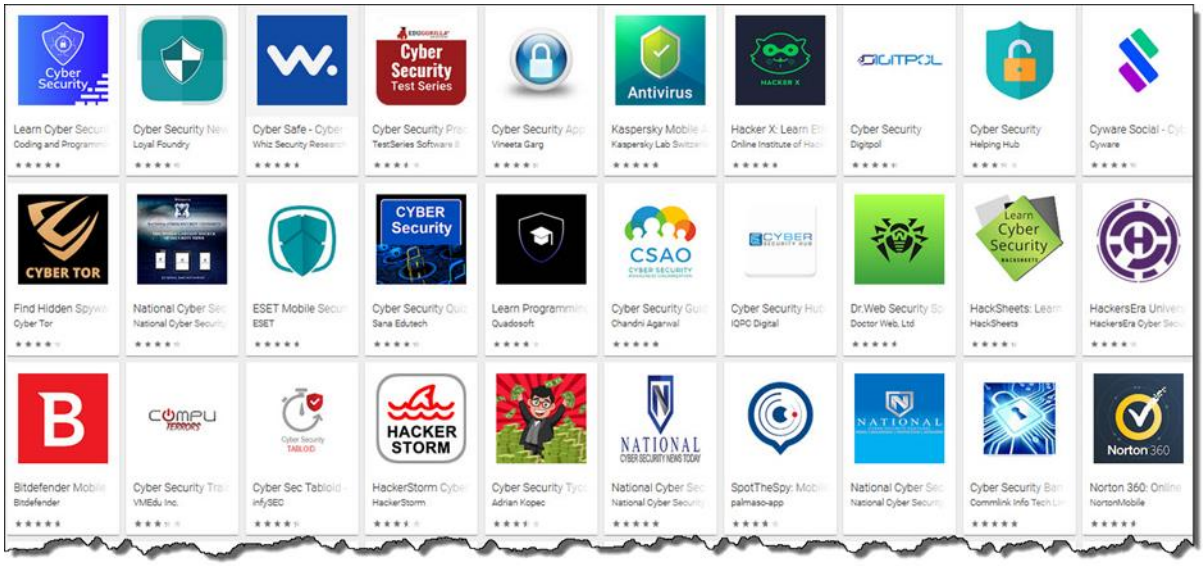

Figure 3: Mobile applications on cybersecurity

Using mobile applications for independent work, the student receives in a convenient compact form additional informational about the means and methods of informational protection, programs for the protection of mobile devices and more. From the given list of mobile applications, which is constantly updated, the student has access to theoretical material on the chosen research topic, can consider a model of a certain process, get an analysis of a certain algorithm, and so on. In Fig. 4, as an example, presents some applications in the field related to data encryption. Applications demonstrate different encryption algorithms, simulate the operation of encryption machines.

Figure 4: Mobile applications for text encryption

Using this application, the student learns the topic of "encryption algorithms," gains skills in encryption and decryption of text.

With the help of mobile technologies, students are involved in a continuous learning and research process that meets modern requirements and does not depend on equipment for access to resources.

4.5. Components of the Learning Environment for Informational and Cyber Security

The NA should provide management of the learning process, planning of learning events, creation and storage of learning materials, organization of communications, verification and analysis of learning outcomes and is created on the basis of learning management systems (Learning Management System,

LMS). Such an environment must be constantly improved through the introduction of innovative learning technologies and the widespread use of open informational and educational space.

Network LE is created using the following tools:

• Learning management based on open LMS MOODLE (or cloud-based LMS Canvas)

• Save training materials using MOODLE, Google Drive or other cloud file storage

• Organization of cooperation using MOODLE, Wiki, Google Docs, Google Sheets, Google Slides or MS Office 365

• Organization of communication via MOODLE, e-mail, forums, video communication systems, virtual audiences: Gmail, Google Chat, Google Meet, BigBlueButton, Zoom, Webex, MS Teams, etc.)

• Knowledge testing using MOODLE, Google Forms, Kahoot and other cloud and mobile tools for tests, quizzes, educational games

• Planning of educational events with the help of MOODLE, Google Calendar

• Training in informational security using open Internet resources Networking Academy CISCO, Microsoft Virtual Academy, mobile applications, augmented reality designers

Education of students with the use of LE is carried out in traditional forms: classes (theoretical training), independent work, practical training, control measures (modular intermediate control, final control). The lecture material is presented in text, graphic and multimedia formats and is stored in the cloud storage of Google Drive files, which allows you to use a flexible system of access to educational resources. LMS MOODLE allows you to integrate cloud services, including videos from Youtube, into training courses to host video lectures. Links to lectures with the appropriate access rights are contained in the e-learning course in the MOODLE system. In addition, knowledge portals and videos of open educational resources are used, which are constantly updated. Thus, a collection of materials is created in the field of study in accordance with the curriculum for each of the content modules. To study certain topics, courses at Networking Academy CISCO are provided with the appropriate certificates.

Long before the advent of COVID-19, universities have gained some experience in conducting remote meetings, departmental meetings, lectures, practical and laboratory classes. This was usually done by using the created virtual lecture audience in MOODLE or video communication systems. The practice of distance learning has shown sufficient quality of communication and high efficiency of training [22].

With the spread of COVID-19 in Ukraine, the introduction of quarantine measures in education and the widespread use of various distance learning platforms, there is a need to consider the functioning of informational and methodological support of educational space in quarantine restrictions. In particular, conclusions were made on the need to expand the existing LE through the introduction of new informational technologies to increase the interest and success of students.

Practical tasks use anti-virus software, informational security services, firewalls, encryption systems, threat and vulnerability detection systems, installation of virtual machines, use of digital signatures, etc. The results of practical tasks are presented in the form of text, tabular reports and presentations using Google Docs, Google Sheets, Google Slides and cloud services for creating interactive presentations (Prezi), infographics (Easel.ly).

Testing and survey services are a convenient means of teacher-student interaction. With the help of such services, each student can form an individual pace of learning and research, to eliminate gaps in training in the chosen field of research. Such services can be divided into two categories, which differ in the way questions and answers are formed, availability and convenience: cloud and mobile. The most famous mobile survey and testing services include Kahoot, Quizlet, Plickers, Easy Test Maker. For example, Kahoot is a free service not only for creating various forms of tests, but also for conducting online quizzes with the help of a special client that is installed on students' smartphones (Android, iOS, Windows Phone). This service allows the teacher to diagnose students' answers and analyze them.

After completing the study of each content module, students undergo intermediate control using test tasks of the MOODLE system, Google Forms and online quizzes using the mobile service Kahoot.

Consultations in the NA were mostly carried out remotely using the MOODLE system, e-mail, discussion, chats, which helps students to overcome the difficulties that arise when studying the material, both in the classroom and independently.

Independent work of students in the NA involved taking the proposed open training courses, such as Microsoft Virtual Academy ("Introduction to security in Microsoft 365"), the use of knowledge portals and videos of open educational.

5. Model of Continuous Step-by-Step Development of the Synthetic Learning Environment on Informational and Cyber Security

Modern LE must be innovative, ICT-rich. Clouds, social tools, mobile technologies, virtual and augmented reality, multimedia technologies have created many opportunities for new learning experiences so that technology has become the highest priority in terms of learning and development. The content of training is shifted towards self-study and project-oriented activities [15].

In general, closed computer-oriented LE situations should gradually become open, personalized, cloud-oriented, mobile, and virtual. As the experience of the authors shows, the improvement and development of emergencies, the introduction of new technologies, forms and means of learning is a continuous process. The model of informational and cybersecurity development with the use of open informational space and innovative learning technologies is presented in Fig. 5.

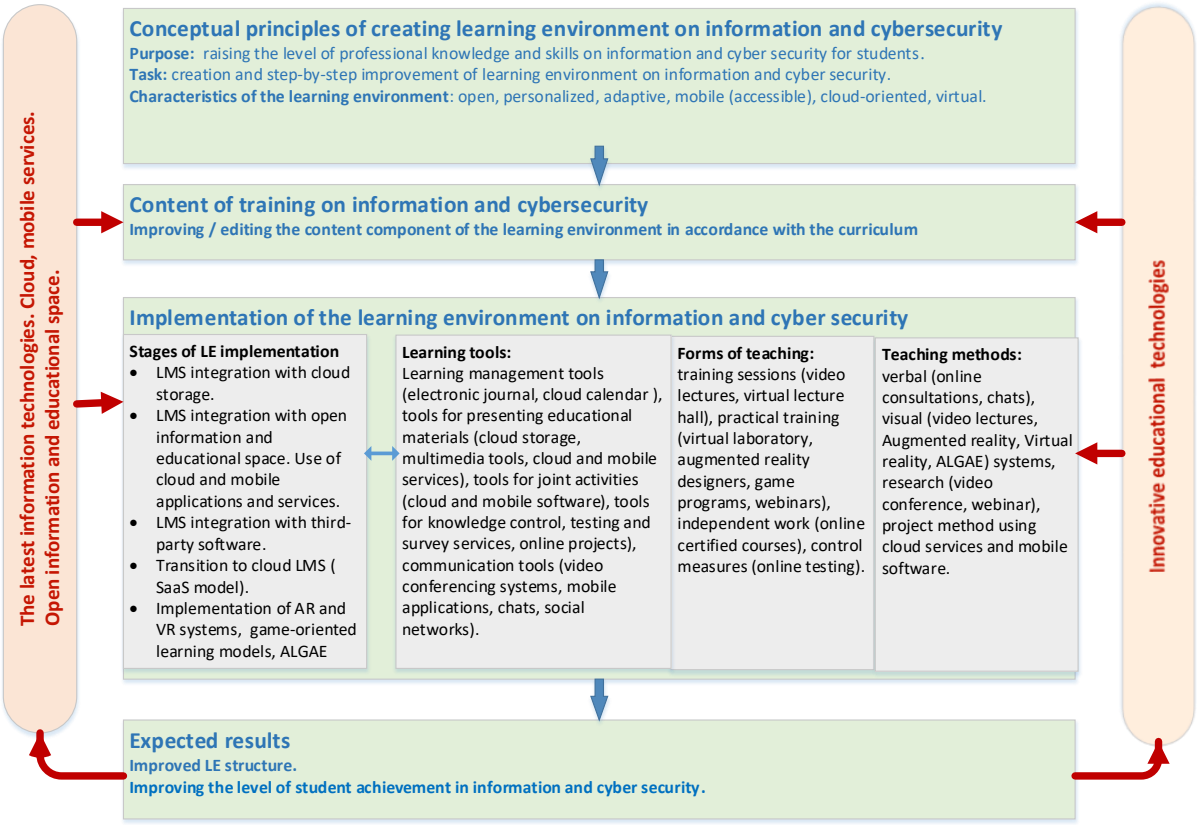

Figure 5: *Model of continuous step-by-step development of LE on informational and cyber security*

For a step-by-step transition to an open modern LE it is necessary:

• Integrate cloud file storage in the LMS to store course materials, such as Google Drive

• Involve in the Internet resources of an open educational environment with opportunities to obtain certificates and access to knowledge portals

• Use mobile applications in the educational process to access the education system, organize communications, professional training, etc.

• Integrate cloud services into LMS for professional training, knowledge testing, presentation of results, etc.

• Expand the functionality of LMS through the use of popular cloud services for teleconferencing, webinars, virtual audiences, online communication, educational and professional communities, etc.

• Integrate LMS with third-party software, for example, with e-learning courses of other LMS, as well as the exchange of training materials between them

• Move the LMS to the cloud

• Use Augmented Reality (AR) and Virtual Reality (VR) systems in the learning process to visualize learning objects and processes. Using game-oriented learning models, ALGAE (Adaptive Learning GAme dEsign) is an adaptive learning model based on theories and practices of game design, learning strategies and adaptive models [15]

The first step may be the use of cloud data warehouses to store course materials, the use of open informational and educational environment to attract online resources from leading educational institutions and companies around the world, the organization of distance learning by creating a virtual lecture hall, mobile applications and visualization technologies, extensive use of cloud services for professional training and presentation of results. This approach to the creation of emergencies is also implemented in the preparation of students majoring in 125 “Cybersecurity” at the University of Kiev named after Borys Hrinchenko [23].

The next step may be the transfer of the educational process management n the clouds, the creation of virtual laboratories for the practical training of future professionals. This will allow you not to install and maintain your own LMS on your own internal resources. Obtaining an appropriate service from the provider according to the SaaS cloud model (Software as a Service) involves the use of LMS, as a Web-platform created by the provider, to manage learning. In this case, all work to ensure the installation, debugging, maintenance and updating of software and hardware is entrusted to the provider. This allows the use of modern LMS even for small educational institutions and individual teachers [20]. There is an integration of Moodle with the cloud version. MoodleCloud is an affordable platform characterized by simplicity, free maintenance, automatic updating of the Moodle version, free use for a limited number of users (up to 50 users) [24]. The MOODLE system was deployed on the cloud server https://moodlecloud.com/ for teaching masters the discipline “Cybersecurity” within the specialty 076 “Entrepreneurship, trade and exchange activities.” Cybersecurity course page in LMS MoodleCloud (https://security.moodlecloud.com/coursr/viewphp?id=3).

6. Analysis of Learning Outcomes and Prospects for Further Research

The survey of students after completing the above courses on readiness to use cloud services, mobile applications, distance learning systems showed that 89% of students rated 4-5 on a 5-point scale the need and convenience of using these technologies in education. Students are motivated to take certified courses in informational and cyber security. The study [17] presents an analysis of the course “Cybersecurity Essentials” of the CISCO Academy, which demonstrates the high performance of students of the group "Innovation Management" (masters).

Students work according to the schedule approved by the teacher, send assignments on time. The teacher has data on the activity of tasks by dates and other indicators.

93.1% of students enrolled in the educational programs "Innovation Management" (masters) and “Economic Cybernetics” (bachelors) have successfully completed courses and received certificates from the Academy of CISCO. The work of 6.9% of students is assessed as satisfactory, and the certificate is not issued. There were no students who received an unsatisfactory grade.

The business world is becoming more global, mobile and digital, so it is necessary to increase the level of training of future professionals, in particular in economics and management in accordance with the needs of digital technologies. In this regard, it is necessary to develop a national strategy for cyber education, ie to deploy a special and general system of cyber education, in particular to pay more attention to the formation of a "culture of cybersecurity" in future professionals in the digital economy.

In accordance with the requirements outlined in the article to the learning environment for informational and cyber security, a method of gradual introduction of new innovative learning technologies using open informational and educational space, mobile learning technologies, cloud applications and services. As a result of the research, the stages of gradual transition from a closed network learning environment to an open, personalized, cloud-oriented, synthetic one are determined. Continuous improvement of the learning environment with the possibility of step-by-step virtualization allows gradually moving to distance learning using virtual classrooms and laboratories, augmented reality technology to build a visual model of learning material that shifts the content of learning towards self-learning and project-oriented activities.

The results of the study showed that the use of the proposed learning environment helps students gain the necessary knowledge, skills and abilities in informational and cyber security, increases the interest and success of students. The use of open learning resources with the ability to obtain certificates, mobile and cloud applications allows students to choose convenient forms and means of learning to gain practical skills in informational security in cyberspace.

We see areas for further research in the introduction of new learning technologies, the development of a learning environment for informational and cyber security for higher education students in the fields of knowledge covering the humanities and natural sciences.

7. References

[1] Cabinet of Ministers of Ukraine. (2021, Mar. 03) Order No. 167-r. On approval of the Concept of development of digital competencies and approval of the action plan for its implementation. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

[2] Digital Agenda of Ukraine – 2020). Conceptual principles (version 1.0). Priority areas, initiatives, projects of "digitalization" of Ukraine until 2020. HITECH office. – Грудень 2016. – 90 с. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.

[3] Cyber Security Breaches Survey 2020. URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

[4] Verkhovna Rada of Ukraine. (2017, Oct. 05) Law № 2163-VIII, On the Basic Principles of Cyber Security of Ukraine.URL: https://zakon.rada.gov.ua/laws/show/2163-19.

[5] I.V. Diorditsa, The state of training of specialists in the field of cybersecurity. Visegrad Jornal of Human Rights 1 (2016) 53– 59.

[6] V. Buryachok, V. Bogush, Yu. Borsukovskyj, P. Skladannyj, V. Borsukovska, Model of training specialists in the field of informational and cyber security in higher education institutions of Ukraine, Informational Technologies and Learning Tools, 5 (2018), pp. 277-291. doi: 10.33407/itlt.v67i5.

[7] I. V. Chychkan, S. O. Spasiteleva, Yu. D. Zhdanova, The educational environment for forming secure base behavior in cyberspace of future professionals in economics and management Informational Technologies and Learning Tools 4 (2021) 354-375. doi: 10.33407/itlt.v84i4.3646

[8] G. Austin, Eds. Cyber Security Education. Principles and Policies. New York, NY, UK and New York: Routledge, 2020.

[9] K. Daimi, G. Francia, Eds. Innovations in Cybersecurity Education. London, UK: Springer, 2020, doi: https://doi.org/10.1007/978-3-030-50244-7.

[10] O. Burov, S. Lytvynova, E. Lavrov, Yu. Krylova-Grek, S. Shevchenko, O. Orliyk, S. Petrenko, O. Tkachenko, Cybersecurity in Educational Networks, in: Proceedings of the 3rd International Conference on Intelligent Human Systems Integration (IHSI 2020): Integrating People and Intelligent Systems, February 19-21, 2020, Modena, Italy, 1131, pp. 359-364. doi:10.1007/978-3-030-39512-4_56

[11] Yu. D. Zhdanova, S. O. Spasiteleva, S. M. Shevchenko, Formation of informational protection competence to students of it-specialties with using .NET FRAMEWORK cryptographic services, Physical and mathematical education. 1 (2019) 48-54.

[12] V. Yu. Bykov, Open learning environment and modern network tools of open education systems, Scientific journal of National Pedagogical Dragomanov University. Series 2: Computer-based learning systems 9 (2010) 9-15. URL: http://nbuv.gov.ua/UJRN/Nchnpu_2_2010_9_4.

[13] A.M Gurzhiy, V.V. Lapinsky, Electronic educational resources as the basis of the modern educational environment of secondary schools, Journal of Informational Technologies in Education, 15 (2013) 30-37. doi: 10.14308/ite000388.

[14] S. H. Lytvynova, Development of educational environment of a comprehensive educational institution as a scientific problem Scientific Bulletin of Melitopol State Pedagogical University. Ser.: Pedagogy. 1 (2014) с. 39-47. URL: http://nbuv.gov.ua/ UJRN/Nvmdpu_ 2014_1_7.

[15] O.P. Pinchuk, S. H. Lytvynova, O. Yu. Burov, Synthetic educational environment – a footpace to new education, Informational Technologies and Learning Tools 4 (2017), с.28-45. doi: 10.33407/itlt.v60i4.

[16] Synthetic Environments for HSI Application, Assessment, and Improvement, STO TECHNICAL REPORT TR-HFM-216. AC/323 (HFM-216) TP/614, 2015.
[17] The results of a survey of students of the Faculty of Economics of KNU, 2019/2020 academic year. URL: http://econom.univ.kiev.ua/wp-content/uploads/2019/12/Результати-опитування-студентів-2019.pdf.
[18] CISCO Networking Academy: Security courses. URL: https://www.netacad.com/portal/teaching.
[19] O.M. Kryvonos, O.V. Korotun, Stages of Designing a Cloud-Oriented Environment in Learning Databases of Future Teachers of Informatics, Informational Technologies and Learning Tools 1 (2018), 130-145. doi:10.33407/itlt.v63i1.
[20] UNESCO Policy Guidelines for Mobile Learning (2013) URL: http://iite.unesco.org/pics/publications/ru/files/3214738.pdf.
[21] Augmented reality in education. VR-Journal | Virtual and augmented reality portal (2017). URL: https://vr-j.ru/stati-i-obzory/dopolnennaya-realnost-v-obrazovanii.
[22] BigBlueButton – Open Source Web Conferencing (2020) Engage Your Online Students: BigBlueButton is a web conferencing system designed for online learning. URL: https://bigbluebutton.org.
[23] Yu. D. Zhdanova, S.O. Spasiteleva, S.M. Shevchenko, The Application of the Security.Cryptography Class Library for the Practical Training of Cyber Security Specialists, Cybersecurity: education, science, technology, 4 (2019), c.44-53. doi: 10.28925/2663-4023.2019.4
[24] L.V. Nozdrina, Innovative CLOUD COMPUTING: Challenges for Education, Journal of Informational Technologies in Education, 1 (2019), 19-50. doi: 10.14308 / ite000691.