Chapter 7 – CYBER SYSTEMS: A POTENTIAL PROTECTIVE AND ORGANIZATIONAL MEANS PERSPECTIVE

Oleksandr Burov
Institute of Information Technologies and Learning Tools
UKRAINE

At present, our lives are being built more and more around digital networks. Interventions to these networks pose a real threat to humans and to the country [1]. In this context, humans should be considered as not only military (including cyber) specialists, but everybody, because the cyberspace becomes the general environment of a human life and activity. For example, Internet of Things (IoT) entered our life practically in each house (computers, laptops and smartphones, routers, IP cameras, digital video recorders, etc.). In 2018, more than 30 billion IoT devices around the world were connected to the Internet.

In order to keep abreast with the rapidly changing threat landscape and maintain a robust cyber defence, civilian and military organizations at the national and international levels try to adopt their new enhanced policy accounting for new challenges [2]. The policy establishes that cyber defence is a part of the core task of government and collective defence, confirms that international law applies in cyberspace and intensifies military cooperation with industry [3].

The top priority is the protection of the communications systems owned and operated by them. Cyberspace is and will continue to be a very important part of the battlefield of ideas and civilizations [4]. Lesson learned from Ukraine-Russia conflict allows to argue that most future operations will (at least) start in cyberspace and operations will most probably be conducted within it during the conflict, increasing the importance of its control [5], [6].

While technical/technological solutions are being developed in response to cyber attacks, there is increasing awareness that the role of human performance and decision making in cyber security is critical to increase the effectiveness of responses to developing threats [7]. Especially it is significant from viewpoint of future manpower, because young people are especially sensitive to external influence and are the most active part of "network population", and "Cognitive space is the goal of any information war, both in peace, for example, during elections and in military situations. In fact, the transmission of information over which everyone is fighting is a secondary goal, since the primary purpose is to change the model of the world in the human brain. You can perfectly transmit messages that do not lead anywhere" [6].

New challenges of time and new directions of society development – Society 4.0, Education 4.0, penetration of the latest technologies into all spheres of life [8], "hybrid" warfare – require understanding of the key and safety issues of the educational process in digital space, in particular the security of all direct participants, the organizers of education, the state, as well as the safety of the content of learning [9]. Accordingly, the significance of cyber security has reached the level of competence in human life safety, has become an integral part of digital competence, first and foremost, all participants in the educational process. These trends in the paradigm shift in teaching impose additional requirements both on subjects of learning (both teachers and students) and on learning resources, especially in synthetic learning environments. Training with the use of technical means, primarily electronic, is becoming more and more usual for modern work, during which external and internal factors affecting person cognitive capabilities, and can suffer because of external vulnerabilities coming from networks. As a result, the training of cyber security specialists has rapidly increased, as their global deficit in the world by 2020 is estimated at 1.5 million workers.

Training of specialists in cyber security is being conducted in hundreds of universities worldwide. Typically, future specialists receive theoretical knowledge and practical skills in programming, developing and managing databases, developing information security models and security policies, technical and cryptographic information security, building secured digital TCP/IP networks and maintenance of public key certificates, testing of penetration protection systems, administration of secure information and communication systems, monitoring and auditing, etc. [10]. However, five years after the adoption of the ISO standard [11], the vision of the cyber security problem has changed significantly, as a person ceases to be the sole subject of cybercrime, turning into an object by itself, and not just its financial and economic interests and opportunities [12]. So, according to the analytical company RAND Corporation, the structure of cyber risk has changed in recent years. More and more analysts pay attention to the fact that the main causes of incidents in Internet resources in 2017 were related to the effect of the human factor, the massive fragmentation of IoT devices and cloud services [13]. Particularly this problem is getting worse by the growing role of social networks in human life in general and in education, in particular, as well as the understanding of the need to transition to education throughout lifespan.

Over the past three years, educational reform has been developed in many economically developed countries by educators, among them developed and presented in the EU. Digital Competence Framework for Citizens 2.0-2.1 [14]. Information and communication competence was defined as one of the key competencies. Cyber security issues were important components of this competence and reflect the common approaches formulated in the Digital Competences Framework for EU citizens [14].

7.1 THEORETICAL AND METHODOLOGICAL QUESTIONS OF THE CYBER SECURITY IN EDUCATION

The human factor may be a system's weakest link, but at the same time it may also be a powerful resource to detect and mitigate emerging threats. Several areas of most critical and urgent needs as well as the knowledge gaps to address in cyber research agendas of NATO and the nations can be defined as psychosocial, cultural, conceptual and organizational dimensions of cyber security.

Cyber objects (humans) can be decision makers, key defence specialists, financial managers, key industry managers, creators of knowledge, and general population (including future military and defence manpower).

Successful cyber security involves accounting for all groups of remedies. Ignoring any of them can lead to loss of government control, military control, financial control, industry control, manpower control, and data.

Taking into account last years' trend in hybrid war, the cognitive war needs a special attention, because its goal is not a prompt military operation and fight for territorial or economic resources, but for people [6]. Moreover, not only the highest level's decision makers, but also the entire population of the target country, since it must perceive and support state leaders controlled by the aggressor (e.g., via mass media), as events in Ukraine and other countries demonstrated over last years. In such a context, cyber security is a way of countering and neutralizing cognitive weapons.

Cognitive weapon is a control of the intellectual environment of the country of the enemy by false scientific theories, paradigms, concepts, strategies, influencing its governance towards weakening the defence of significant national capacities [15]. Main features of the cognitive war are as follows:

- *Military strategy* is suppressed and subordinated the consciousness of the enemy. Opponent is programmed cognitively to self-destruction.

- *Goal* is implanting to the enemy a thought that the struggle itself does not exist.
- *Result* consists in enemy's cognitive damage which features can be characterized as:
  - Represented false theory affects national science, relevant scientific schools and generations;
  - Corresponding defective frames are programmed to misconceptions about the most important management paradigms, development of the country;
  - This reproduce generations of students and graduate students of the corresponding grade; and
  - They saturate the relevant reference structures of government and decision makers, accordingly, there is an erroneous destructive state management policy.

To date, there is a gap between the traditional approach to cyber security (the solution of technical and information tasks) and the need to take into account the human factor in the cognitive dimension. Understanding of this leads to changes in the training of specialists in cyber security : in their training programs, more and more skills and abilities are added with focus "on the social, economic, and behavioural aspects of cyberspace, which are largely missing from the general discourse on cybersecurity" [16], p. viii, that needs to take into account the human features and his/her functional state as well as cognitive resilience, because of increasing role of the cognitive warfare [17].

The closing of such a gap needs to expand the number of key Cyber Security (CS) questions: Who, Why, What, Where, When, In What Way?

Besides, selection of appropriate CS means should take into account their time perspective:

1) *Short-term* (cyber attacks, battle operations);

2) *Middle-term* (cyber staff training); or

3) *Long-term* (cognitive weapon).

The issues of cyber security are acute from the time that computer technology has ceased to be just the prerogative of major research centres. With the advent and spread of local and global networks, the understanding of cyber security, relevant trends, problems and challenges has changed. Let's consider them taking into account the transformation of education in the direction of digital education, Education 4.0.

7.2 INFORMATION AND COMMUNICATION TOOLS AS THE BASIS FOR THE EMERGENCE OF A CYBER SECURITY PERSPECTIVE

To date, our lives are building more and more around digital networks, and virtual media is becoming a new social environment [18]. Interference with these networks poses a real threat to security in education and the country as a whole. The constituents (factors) of the network can be represented in this simplified form (see Figure 7-1).

Network agents can act as nodes – people (resource creators and their content, resource administrators, regular or random users), technical (terminal stations, computers, networked gadgets, communicators) and information (databases, databases knowledge, control systems, etc.) means. All agents, depending on their nature, have their own interfaces and types of communication with other agents.

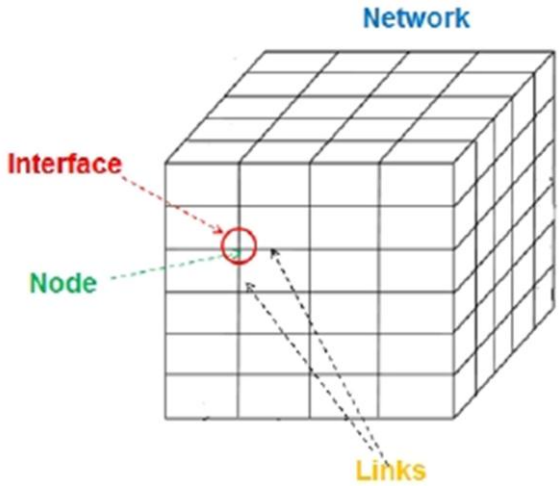

Figure 7-1: Simplified Model of Cyberspace.

However, it should be noted that the network ceased to be merely an intermediary between users (means of communication in time of the development of technologies for building networks), their complication, the use of artificial intelligence, the emergence of cloud and foggy technologies, the growth of the power of Databases (DB) and Knowledge Bases (KB). Since the information in the global network exists outside the defined space and time, the network itself becomes an active agent of human influence [12], first of all, while maintaining large amounts of data available to the public [19]. Any user can log on to the network (legally or illegally) and access the necessary nodes (when using cloud-based means, specific nodes may not be known to the common user), including changing their content (for example, a Wiki-object) for permitted rules.

However, information in DBs and KBs under the allowed rules can be changed or introduced in order to distort the representation of users about the data they are looking for. Certain users are able to use it to influence the broad or target audience, "distorting" the nodes (technical or informational) or influencing them by means of social engineering (if the node is a person). Since the network is a system of connected nodes, a damaged ("distorted") node may already effect on its secondary nodes. In addition, distorted information begins to exist on the network, even independent on the person ("aggressor"), who introduced it (Figure 7-2).

Thus, the network acquires the features of an independent component (factor), which affects its properties, functioning and users, as well as the System "Human-Technology-Environment" (SHTE) as a whole. All four network performance parameters (see Figure 7-1) have certain common critical properties from the point of view of efficiency and impact on the user – initiative, efficiency, stability, flexibility and performance (Table 7-1). Their manifestation in relation to each factor can be characterized by certain indicators, characteristic for the corresponding parameter, and a set of indicators allows estimating the overall influence of the factor on the network as a system "human-technology-environment".

Any consideration of cyber security as an independent factor in SHTEs is limited and only partially effective, since it does not take into account the changes that occur with SHTE agents, not only in time but also in space, and this effect expands with the development of technologies from local to global ones. Corresponding changes occur in relation to the learning environment.

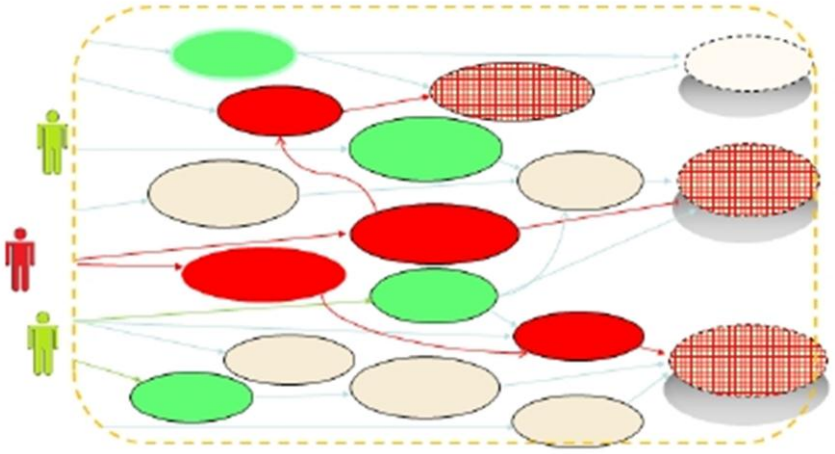

Figure 7-2: Example of an Active Fragment of the Network and External Users (Green – Normal, Red – "Aggressor") Connected to Nodes (Red – the Node with "Distorted" Information).

Table 7-1: Network Elements and Their Features.

HSI Features	Node	Interface	Link	Network
Initiative	Situation awareness	Situation information	Routing	Intent
Efficiency	Performance	Usability	Packet loss	Quality of service
Stability	Response to stress	Consistency	Reliability	Resilience
Agility	Capability	Display modes	Redundancy	Reconfigure
Capacity	Workload	Clutter	Bandwidth	Density

7.3 LEARNING ENVIRONMENT AND CYBERSPACE

The Educational Environment (EE) is one of the cornerstones of education. There are many different definitions and classifications of the EE. It has a multifactorial influence on subjects of the educational process, changing both in time and in space. And this is true both for the traditional learning environment and for the synthetic one. One can note that the learning environment in the content plan always arises as a dynamic process of forming a network of relations in the subject of learning, to which (not always consciously) selectively involve the various elements of the external and/or internal environment, and this dynamic process is characteristic of any learning environment, but in immersive and virtual EE, it becomes even more acute due to a more profound immersion of the student into the learning process.

Different authors distinguish natural and artificial, subject and informational dynamic, adaptive and other educational environments, using different criteria of their typology; for example, the style of interaction within the environment, the nature of the attitude to social experience and its transfer, the degree of creative activity, and by nature interaction with the external environment. However, at present, the digital space or cyberspace is the main attraction due to the exacerbation of the human security problem in it, first of all, the young person whose formation takes place only in the personal and competent dimensions.

Attention is drawn to the fact that cyberspace is determined by the diversity of compounds, which simultaneously translates it into a category of risk area. All increasing dimensions, coverage and functions increase the capacity of both law-abiding citizens and hostile players. An opponent only needs to attack the weak link of the network in order to win a new bridgehead and gain advantages [7]. Local issues can grow and spread rapidly, creating threats and systemic risks. The vulnerability in the cyberspace is real, serious and it is growing rapidly. Facilities of special importance infrastructure, intelligence, communications, command and control, trade and financial operations, logistics, mitigation and emergency preparedness are entirely dependent on IT systems integrated in the network. Violations of cyber security, theft of data and intellectual property do not know the boundaries. They affect everything from personal information to state secrets.

Cyberspace can be considered as a triad, which includes:

1) Information in its digital representation: static (files recorded on the storage medium) and dynamic (packets, threads, commands, queries, etc.);
2) Technical infrastructure: Information and communication technologies, software, databases and knowledge bases; and
3) Information interaction of entities using received (transmitted) information and processing through technical infrastructure.

This notion is bound with the notion of cyber security as the protection of the vital interests of man and citizen, society and state when using cyberspace. At the international level, a number of definitions of this concept are used, but accounting the fact that learning is a type of activity, one can agree with the approach that cyber security is considered as “any networking, digital activity, including the content of information and activities that are carried out through digital networks” [20]. Keeping in mind that today’s students are born in a digital age, grow, study and develop to a large extent precisely in cyberspace, one can argue that cyberspace is and will remain a very important part of the battlefield of ideas and civilizations. Accordingly, before education there are new tasks connected not only with the formation of the necessary knowledge and social awareness of the learner, but also his/her understanding of his/her own integration into the world community already in the early stages of learning, practically unlimited possibilities of the influence of cyberspace on personality, responsibility to him/herself and society for their own behaviour and its (possible) global implications, knowledge and understanding of the dangers of cyberspace.

7.4 THREATS TO PARTICIPANTS IN EDUCATIONAL PROCESS FROM CYBERSPACE

The threats’ spectrum from open cyberspace is constantly expanding. If ten years ago the hazard to schoolchildren could be reduced to a relatively small number of groups (viral attacks, cybercrime, threats of Internet surfing), at present, the diversity of threats and hazards is constantly increasing, affecting all possible human actions in the network. The greatest danger to students is hidden active threats [21].

To protect young humans from cyber threats especially their cognition, it is useful to understand modern trends in education (digitalization of education) and potential specific targets of attackers in educational domain. Recognizing the role of education subjects and their specific role in society, various aspects of the education domain were captured and reflected throughout the ontology as shown in Figure 7-3 with red ovals circling the relevant concepts. For example, one of the threat vectors in the ontology is policy and procedural non-compliance and one of the mitigation mechanisms is policy management.

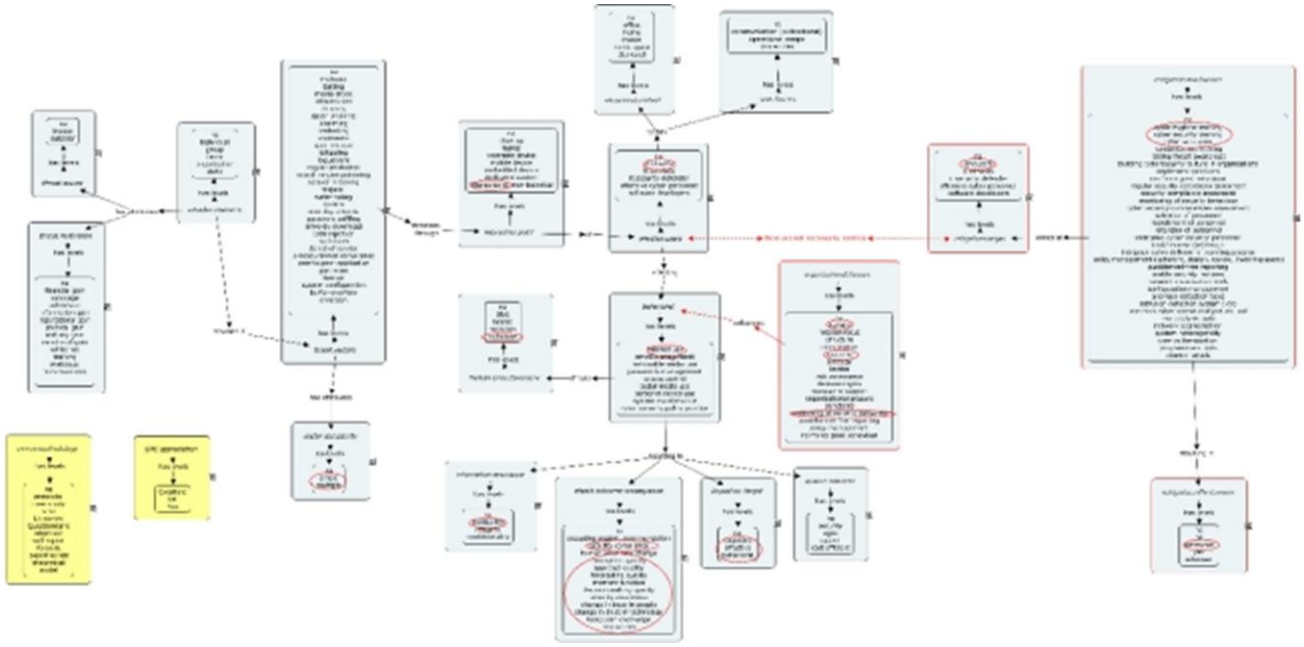

Figure 7-3: Education Aspects Captured in the Framework. See Annex A, Figure A-1 for full size non-annotated image.

Section 7.4 summarises general factors related to human-systems security related to education and provides an overview of the relevant literature.

7.4.1 Network Threats

The active use of networks, especially by children and young people, is accompanied by an increase in various types of threats coming from the Web. This problem is especially acute when developing and using social networks. The most active hidden threats (for children) originating from a computer network can be represented by the following classification [21]:

- Viral attacks;
- Cybercrime (spamming, carding, phishing, botnets, etc.); and
- Threats from network surfing (cyber bullying, "adult" content, illegal content, online violence, private disclosure, paid services, etc.).

The authors recommend to consider the interaction of students between them and students with the computer network as a system "human-technology-environment." In this system, the computer network acts as a machine, which allows us to consider the impact of the network on a person as a threat from the machine. Accordingly, the concept of "network effect" can be detected through the notion of "operator error and low quality of the operator", "the impact of computer games" and "Internet addiction."

The threats coming from networks can be divided into the following types: active and passive, open and hidden, current and deferred ([21], p.308).

Using the ergonomic approach and methodology, it is possible to evaluate active threats as a hierarchical set of indices:

- One *integrated* (complex) index: the level of hazard due to the operation of the computer network. The index is the dimensionless value included in the estimates of the system of the upper level.
- Three *group indicators*: the level of danger caused by viral attacks, cybercrime and internet surfing. Indices are dimensionless values and are associated with the average level of system evaluation.
- Set of particular indices of a group of one or a combination of threats. Indices are also dimensionless and correspond to the classification of lower-level systems.

Such an integrated index gives an opportunity to assess the influence of the set of weighted threats independently on their nature and ways of measurements, and to project it on a scale [0,1] that could be a scale of the general cyber risk. For example, 0 … 0.2 means lack of significant risk, 0.2 … 0.5 the presence of risk, 0.51 … 0.8 high risk, > 0.8 unacceptable risk.

7.4.2 Cyber Security (CS) Directions

As a rule, national legislations related to CS do not consider the sphere of education as the critical area for the protection of which they are aimed. However, today's pupils and students in the short term can work in those areas. Therefore, they already need protection and appropriate training as well as an understanding of the general possible target groups of cyber security. For example, by the following classification [12], [9]:

- Pupils/students;
- Teachers;
- Children/youth (in general); and
- Population (in general, as a social environment).

Depending on the means of action, the problems (and appropriate means) of cyber security can be classified into five groups:

- Legal;
- Technical;
- Information;
- Organizational; and
- Psychological.

The legal and technical issues of cyber security are handled by appropriate specialists and organizations, so they are not addressed in this article.

Information tools can be categorized according to the tasks solved by the users:

- Protection/Remedies;
- Informing;
- Content;

- Learn how to use;
- Security;
- Lifespan; and
- Avoiding threats.

In the broadest sense possible, *targets* for the impact of cyber security (in addition to critical infrastructure objects) can be:

- Databases;
- Personal data, including financial;
- Mass media;
- Social networks;
- Education/training; and
- Textbooks, historiographical editions.

The latter two points relate to the domain of cognitive safety, i.e., to the prompt human factors area.

Organizational tools for solving cyber security issues are:

- Informing;
- Learning the culture of cyber security, professional staff of CS and the general population;
- Creation of special means of the CS;
- Distribution of CS facilities; and
- Control of use.

Psychological means can be grouped depending on the personal and interpersonal level:

- National;
- Public;
- Group;
- Individual;
- Cultural;
- Cognitive;
- Intellectual; and
- Habits.

Although technological solutions are developed in response to cyber attacks, awareness is growing that the role of human activity and decision making in the field of cyber security is crucial for increasing the effectiveness of responding to emerging threats. This is especially important in terms of future workforce, since young people are particularly sensitive to external influences and are the most active part of the "network population."

The human factor may be a systemic weak link but can also be a powerful resource for identifying and mitigating emerging threats. Several areas of the most critical and urgent needs and gaps in knowledge that are considered in cyber research programs in NATO and other countries can be identified as: psychosocial, cultural, conceptual, and organizational aspects of cyber security.

7.5 POSSIBILITIES AND WAYS OF PROVIDING CYBER SECURITY PROFESSIONAL EDUCATIONAL PROCESS

Recent studies on cyber security show that information technology in this area is constantly being improved and hacker attacks are reoriented not to technology, but to humans (see, for example, https://www.computerweekly.com/news/252448101/People-top-target-for-cyber-attackers-report-confirms). It is especially important to take into account the acuteness of the issue of its personal security and the results of its activities. When a human is "opening" during the work (connecting his/her own information models with the information flow), the information environment becomes not only a subject, but an object and a tool of the activity of other participants in the information space. The information can affect the target human from outside, because the human openness is a result of the goal of work: using information as an instrument, a person has to "touch" it, contact it. At this moment, the human becomes open to information and vulnerable to it.

7.6 SOCIAL ENGINEERING AND CYBER SECURITY

The shifting of the goals of cybercrime from technical (information) to the human link of the SHTE led to the emergence of Social Engineering (SE) as methods and technologies for obtaining the necessary access to information based on the peculiarities of the psychology of people, in particular, the manipulation of human fears, interest, or trust [22].

The main types of social engineering at the time can be considered in relation to education as follows: pretexting, phishing, Trojan horse, *Quid pro quo*, road apple, biting, reverse social engineering, friendly letters, whishing, contacts [23].

Social engineering tools have been widely used in recent years to influence decision makers in politics and business. Recommendations, methods and means of counteracting them are developed and improved (https://lab.deiteriy.com/#service). However, there is virtually no discussion of action and countermeasures in the SE on the educational field, despite the fact that children and teenagers are increasingly exposed to attacks via the Internet, and the use of countermeasures for adults can be extended to pupils/students, but taking into account peculiarities – age and spheres of activity. A lot of tools for SE are proposed for everybody in the Internet (e.g., http://www.spy-soft.net/social-engineering-toolkit/).

7.7 LEARNING SUBJECTS AND SECURE INTERNET

The main way of protecting from the methods of social engineering is to teach Subjects of the Educational Process (SEP). All of them (students, educators, and trainers) should be warned about the risk of disclosure of personal information and confidential information, as well as ways to prevent data leakage. In addition, each SEP, depending on the place and function in the educational process, should have instructions on how and on what topics it is possible to communicate with third parties regarding personal characteristics, which information can be provided to the technical support, as well as what information can notify the learner to third parties and media In addition, you can select nine typical rules of resistance to the SE (https://efsol.ru/articles/social-engineering.html).

Intended user credentials are the property of an educational institution. All employees on the day of recruitment should be told that those logos and passwords that they have been given (if any) cannot be used for other purposes (on websites, for personal mail, etc.), to transfer to the third person or other employees who do not have this right. For example, very often on leave, an employee can transfer his authorized data to his colleague in order to be able to perform some work or look at certain data at the time of his absence. Personal data from the results of testing and performing psychological and medical examinations can be used by SE users; therefore, they require careful use.

Introductory and regular training of staff and students aimed at raising awareness of information security is required. Conducting such briefings will allow the SEP to have current data on existing methods of social engineering, and to not forget the basic rules of information security.

It is mandatory to have security regulations, as well as instructions that the user must always have access to. Instructions should describe the actions of the SEP in the event of a situation. For example, in the regulation you can prescribe what you need to do and where to contact when you try to invite third parties to receive confidential information or credentials.

The computer users should always have current antivirus software, and also install a firewall.

7.8 "COGNITIVE VACCINATION"

On December 20, 2002, the General Assembly of the United Nations adopted Resolution 57/239 Elements for Creating a Global Cybersecurity Culture, which identified nine fundamental complementary elements that form the global cyber security culture [24]:

1) Awareness;

2) Responsibility;

3) Response;

4) Ethics;

5) Democracy;

6) Risk assessment;

7) Design and implementation of security measures;

8) Security control; and

9) Revaluation.

These elements relate to all five groups of means specified in Section 7.4.2 – information (numbers 1, 6 and 9), technical (3 and 7), organizational (5 and 8) and psychological (2 and 4). At the same time, it can be noted that psychological means (which directly relate to each individual) provide only behavioural aspects – responsibility and ethics, that is, manifestation of a person's social attitude towards cyber security. However, in the cognitive aspect, which is shaping in relation to human behaviour, attention is not focused, that is, a person is seen as a relatively passive element of the cyber security system. At the same time, since no means guarantee 100% protection of the person, it is expedient to determine the range of possibilities of the person himself to the formation of personal protection, except for the above.

The analysis of the programs of educational institutions in many countries showed that in studying the teaching methods of learners enough attention to the question of the formation of critical thinking students in connection with the use of the Internet is not always paid [25].

At the same time, solving the problem of the safety of students online in the developed world, where the Internet is widely used in educational and scientific activities, is characterized by an integrated approach and the security problem is closely linked with questions of forming the student's own responsibility for their actions or inactivity on the network to avoid and/or risk reduction. For example, students from the United States, Germany, Canada, Finland and other countries, together with parents and school representatives, sign special agreements on safe and responsible use of the Internet. In such agreements, bonds of safe and responsible use of social networks by all participants in the educational process are defined and prescribed.

The most effective way to deal with the problems of cyber threats is to understand their essence and change their behaviour. Safety rules are simple and well known; they need to be applied. First of all, it's worth looking into actions and understanding what dangerous actions you and other SEPs do. For example, click on the links, relying on the fact that antivirus protection will provide cyber security? Unfortunately, no technical equipment from the cyber security arsenal is a guarantee, especially if the target of the hazardous action is a person as such.

In a cyber-threatening world, an important part of the training of all networking participants should be taken on the possible impact of the cyber environment. General and specific information about cyber threats and possible consequences of their impact on life and human activities should be supported by simulation of certain situations that may occur to the user of the Internet. Effective means of educating teachers and students of safe and responsible behaviour when using Internet resources is to conduct special training sessions on the critical assessment of the reliability of sources and the reliability of data published on the network.

The most effective approach is to use computer simulation of cyber threats in relatively closed systems: corporate and educational ones. As recommended by professionals, if you are dealing with security issues, "training" attacks, in fact, is a useful way. "But it should be used correctly. Not just divide employees into those who felt the trick and those who got caught. It is imperative to convey to others the essence of their mistakes and how not to make them in the future. You can also find out exactly how dangerous the testers have been identified. Perhaps from this you will be able to glean useful ideas" (accessed 03/28/2020 https://legal-it.club/kiberbezopasnost-chelovecheskij-faktor/). Examples include simulation of unauthorized distribution of private information about a particular person in a modelling environment (using real information from social networks, which many do not randomly place there); phishing modelling, etc.

As it is virtually impossible to provide full protection, it is important to train the users' resilience to cyber threats, that is, learning "cyber survival", which consists of the ability to recognize the threat or possible dangerous effect of the network and rational compensation for this action – both psychological and behavioural (including the appeal to the relevant specialists, because of the impossibility of self-restored actions at the initial stage of training). To some extent, such training is similar to the training of first aid measures in the event of damage to health.

Integrated training in these areas can be considered "cognitive vaccination", that is, the formation of a conscious sensory experience of staying under the influence of cyber threat and counteraction to it. In general, the following levels or "layers" of cyber security can be identified:

- Legal;
- Technical;

- Information;
- Organizational; and
- Psychological, with special regards to cognitive means and responsible behaviour.

It is possible to effectively solve the issue of cyber security only if system resources are used at all structural levels, considering the specific weight of each of them for a specific target group and/or the scope of application of the corresponding anthropocentric system.

7.9 CONCLUSIONS AND PERSPECTIVES FOR FURTHER STUDIES

1) The problems of cyber security are not limited to the technical aspects of the protection of information resources; they must include in their entirety the following types of protection: legal, technical, informational, organizational and psychological.

2) At the same time, among psychological means of securing cyber security it is expedient to distinguish cognitive, since the population in general, and especially children and youth, are increasingly becoming targets of cyber attacks, first of all, their cognitive sphere, becoming the most vulnerable (weak) link in the network.

3) The network itself acquires new properties, acting as an independent vector (in addition to factors such as the network node, interface and nodes) in human-centric networks, which make up an ever-increasing share among common networks.

4) Threats to participants in the educational/training process on the part of cyberspace should be considered as passive and active, developing adequate means of protection and viability of the system “subject of educational process – learning – environment”.

5) The most significant for the participants among cyber threats of the educational process are methods of social engineering, whose knowledge and opposition can be most effective in providing cyber security.

6) As part of the training of participants in the educational process on cyber security, it is proposed to use “cyber vaccination”, that is, the formation of a conscious cognitive experience of staying under the influence of a cyber threat and counteracting it as a system of training activities that include, in addition to traditional methods, training “cyber attacks”, as well as the formation of knowledge and skills of sustainability (recovery) in relation to cyber threats.

7) Further research of the problem should focus on the detailed development of types of threats to the participants in the educational process, as well as methods of counteraction. A special point should be the issue of resistance to cyber hazards, which can use the experience of training operators of the emergent industries, primarily diagnosing the current state of the person and necessary adjustments in order to optimize its activities.

7.10 REFERENCES

[1] Nemchynova, K. (2015). Cyber security and cyber weapons as a challenge to the State of Ukraine. https://www.liga.net/economics/opinion/kiberbezopasnost-i-kiberoruzhie-kak-vyzov-gosudarstvu-ukraina-3999533. Accessed 28 March 2020 (in Russian).

[2] Glaspie, H.W., and Karwowski, W. (2018). Human factors in information security culture: A literature review. In: D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, Vol. 593. Cham, Switzerland: Springer.

[3] Schmitt, M.N. (2015). The law of cyber targeting. The NATO CCDCOE Tallinn Papers. Tallinn Paper No. 7. Tallinn, Estonia: CCDCOE.

[4] Snegovaya, M. Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare. www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf. Accessed 28 March 2020.

[5] Gery, W.R., Lee, S., and Ninas, J. (2017). Information warfare in an information age. Joint Force Quarterly. I. 85.

[6] Pocheptsov, G. (2017). The war in cognitive space. Retrieved from https://nesterdennez.blogspot.com/2017/08/global-permanent-war_39.html (in Ukrainian).

[7] Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., and Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cyber security judgment? Computers in Human Behavior 84:375-382, ISSN: 0747-5632.

[8] Bykov, V.Yu. (2018). Knowledge society and education. Retrieved from https://www.youtube.com/watch?v=cDIytlESUz4.

[9] Bykov, V.Yu., Burov, O.Yu., and Dementievska, N.P. (2019). Cybersecurity in digital educational environment. Information Technologies and Learning Tools 70(2):313-331.

[10] Bystrova, B. (2017). Comparative analysis of curricula for bachelor's degree in cyber security in the USA and Ukraine. Comparative Professional Pedagogy 7(4):114-119.

[11] ISO/IEC 27032:2012. (2012). Information technology – Security techniques – Guidelines for cyber security.

[12] Burov, O. (2016). Educational networking: Human view to cyber defence. Information Technologies and Learning Tools 52:144-156.

[13] SecurityLab. Retrieved from https://www.securitylab.ru/news/492191.php. Accessed 28 March 2020.

[14] Digital Competences Framework for EU citizens. Retrieved from https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-21-digital-competence-framework-citizens-eight-proficiency-levels-and-examples-use. Accessed 28 March 2020.

[15] Bagdasaryan, V. (2016). "Cognitive weapons" as a tool for desuverization. Retrieved from https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

[16] Ahram, T., and Karwowsky, W. (2019). Advances in human factors in cybersecurity. In: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24 – 28, 2019, Washington DC.

[17] Bienvenue, E., Rogers, Z., and Troath, S. (2018). Cognitive warfare. Retrieved from https://cove.army.gov.au/article/cognitive-warfare.

[18] Burov, O. (2014). Virtual life and activity: New challenges for human factors/ergonomics. In: Symposium Beyond Time and Space STO-MP-HFM-231, STO NATO, 8-1 to 8-8.

[19] Mansour, R.F. (2016). Understanding how big data leads to social networking vulnerability. Computers in Human Behavior 57:348-351, Elsevier Ltd.

[20] Klimburg, A. (2012, December). National Cyber Security Framework Manual. NATO CCD COE Publications. Retrieved from https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/. Accessed 28 March 2020.

[21] Burov, O.Yu., Kamyshin, V.V., Polikhun, N.I., and Asherov, A.T. (2012). Technologies of network resources' use for young people training for research activity. Monograph. Burov, O.Yu. (Ed.), Kyiv: TOV «Informatsiini Systemy» (in Ukrainian).

[22] A powerful tool for social engineering. The WordPress Security Learning Center: Understanding Social Engineering Attacks. Retrieved from https://www.wordfence.com/learn/understanding-social-engineering-attacks/. Accessed 28 March 2020.

[23] Savchuk, T. (2018). Social engineering: How fraudsters use human psychology on the Internet. Accessed 30 August 2018. Retrieved from https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html (in Ukrainian).

[24] Elements for creating a global cybersecurity culture. UN document. Retrieved from http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml. Accessed 28 March 2020.

[25] Dementiievska, N.P. (2015). Formation of the skills of critical evaluation of web resources and the problem of student safety on the Internet. Kompiuter u shkoli ta simi 7:46-51 (in Ukrainian).