Vulnerabilities of Cyber Security of Technical Intelligentsia in Relation to Social Engineering

Vladimir Kononovich [1], Irina Kononovych [2], Oksana Shvets [3]

[1, 3] *State University of Intelligent Technologies & Telecommunications, Kuzneshnaya str. 1, Odessa, 65021, Ukraine*
[2] *National Academy of Food Technologies, Dvoryanskaya str. 1/3, Odessa, 65023, Ukraine*

Abstract

In the field of cybersecurity, the most critical problems are with the human factor and, in particular, the problem of cyber protection of individual and collective consciousness and subconscious. The objects of cyber defense against social engineering, among others, are the individual and collective consciousness and the subconscious. Uncontrolled influences of social networks can have serious consequences for civilization and culture. The causes of vulnerabilities are the peculiarities of the functioning of social networks and the processes of information perception and thinking. Information technology and objective factors of thought processes turned out to be unprotected. Due to the high complexity, some of our models of reality are not based on knowledge, but on faith. The rest of the models can be based on the subconscious. Collective consciousness has certain vulnerabilities due to conflicts. Educated technical intelligentsia falls under some vulnerabilities more than ordinary people. Cognitive distortion "**myside bias**" forces us to remain faithful to our own worldviews and those of our group. Protection from the trap of distortion is a critical attitude towards yourself and your views. Only this will help us not to get stuck in the "trap of distortion". It must be understood that belief is a conditioned reflex of the mind, a habit, a stereotypical reaction of understanding, an explanation of the situation when a certain stimulus appears. You can work with conditioned reflexes. They can be installed and removed at will. To counteract the automatic reaction and conditioned reflexes, it is recommended to analyze the origin of beliefs, their inconsistency, adequacy and impact on activities.

Keywords

Cybersecurity, cyber defense, social engineering, individual consciousness, collective consciousness, cognitive distortion, socio-psychological methods, mathematical model, logical-linguistic model.

1. Introduction

Software and technical, organizational, cryptographic, technical, organizational and technical measures and means of cybersecurity have been significantly developed. Norms, rules, best practices are developed. At the same time, the situation with the human factor remains unsatisfactory. The share of anthropological problems with information and cyber security today reaches 85% or more [1]. One of the main reasons is the use of social engineering. Aspects of this problem are the subject of research.

There are an extremely large number of publications on this topic. It is difficult to make a comprehensive review. An informative review of methods of influencing humans was provided by Alexander Wentland [2]. We will add an analysis of some of the latest publications. In [3] the ontology and examples of application of knowledge on social engineering in the field of

ISIT 2021: II International Scientific and Practical Conference «Intellectual Systems and Information Technologies», September 13–19, 2021, Odesa, Ukraine
EMAIL: vl_kononovich@ukr.net (A. 1); irinakononovich2020@gmail.com (A. 2); ovshvets@ukr.net (A. 3)
ORCID: 0000-0003-2720-3337 (A. 1); 0000-0001-7146-3692 (A. 2); 0000-0001-6860-7894 (A. 3)

cybersecurity are presented. Based on an interdisciplinary view of social engineering [4] provides practical recommendations for research.

Other publications consider the assessment of familiarity with social engineering in the education sector [5]; strategy of social engineering attacks on information resources [6]; modern solutions, measures, policies, tools and applications for cybersecurity and social engineering [7]. Recommendations and best practices for counteraction are reflected in the standards, for example, in ISO / IEC 27032: 2012. A popular book among domestic publications [8], which conducts a systematic analysis of social engineering.A popular book [8] provides a systematic analysis of social engineering.

Researchers In the media, scientists report "that people's lack of understanding of how social networks affect us is a danger to democracy and scientific progress." Surprisingly, this also applies to the educated technical intelligentsia. In addition, operators and providers are unable to stop misinformation. "The authors warn that if such facts are left misunderstood and out of control, we may see unintended consequences of new technologies that contribute to phenomena such as elections, disease, violent extremism, famine, racism and war." Counteraction is complicated by the fact that, as indicated in 1999, Rastorguev S.P. [9], perfect information wars are being waged. In the considered publications the phenomenon of easy vulnerability to certain types of attacks on a certain social group of people remains unclear. Specifically, it is a question of cognitive distortion "myside bias", which affects the educated technical intelligentsia [10].

The purpose of this work: to provide a logical explanation of the phenomenon of significant vulnerability of individual and collective consciousness and subconscious from the attack of "cognitive distortion", myside bias, a certain social group of people, namely - a highly educated part of the technical intelligentsia - and make recommendations on methods and means attack.

Research methods - logical-linguistic and heuristic modeling.

To achieve this goal the following tasks are solved:

1. Analysis of modern characteristics of individual and collective consciousness and subconscious.
2. Modeling of methods of perception and processing of information by the person.
3. Consideration of the peculiarities of the functioning of individual and collective consciousness.
4. Development of recommendations for counteracting attacks such as "cognitive distortion".

2. Characteristics of individual and collective consciousness and subconscious as objects of cyber defense. Modern views

At the end of the twentieth century, a new science was born – "Infodynamics, which deals with the most general laws in the processes of transmission, transformation, processing and storage of information (or its related type of negentropy)." In particular, the theory of infodynamics sets out the main provisions of the negentropic theory of mental activity of man and society. This section considers some of the provisions based on a sample of materials from the work of E.Kh. Live [11].

One of the initial tenets of infodynamics is the following: "Consciousness, thought, science and other results of mental activity of man and society are secondary reality (now spread a broader term – virtual reality), ie approximate models of the real world. However, they are also objectively existing systems consisting of matter, energy and negentropy. Consciousness is determined by a set of models with the maximum possible entropy, part of which is compensated by negentropy. Approximate models are thoughts, emotions, subconscious, perception, religious views, which are also objective systems subject to cyber defense. Let us take into account that modern science is the brainchild of religion and began its development under the wing of medieval religion.

Man and science create simplified models-systems for solving problems, in particular thoughts, concepts, theories, etc. Every model that a person imagines in his mind is a system in virtual reality (in the brain). The primary reality of human thought is not reflected exactly.

Primitive logical-linguistic and mathematical models of informational influence on consciousness by the authors were considered in [12]. The science of semiotics, the theory of sign systems, and its sections deal with the qualitative and value side of information; syntax – the study of formal relations between signs; semantics – the content of information; pragmatics – the question of determining the value of information.

The main task of collective consciousness and science is to manage global processes associated with the change (increase or decrease) of generalized entropy (GE) and generalized negentropy (GNT) in the noosphere and associated with the development of human civilization. If the total increase in GE in global systems exceeds the total increase in GNT, then the world is dominated by the processes of destruction, movement towards chaos and uncertainty.

Ultimately, this could lead to the destruction of an entire civilization and culture. Therefore, the accelerated growth of GNT in comparison with the growth of GE must be ensured. Advances in science and technology can fall into the hands not only of honest, conscientious people, but also of criminal organizations.

Consider the principles of information reception, important from the point of view of cybersecurity.

In any system there is a general principle of self-regulation of systems. The principles of saving negentropy, minimum energy dissipation potential, minimum energy consumption and negentropy, etc. are formulated.

Man, as a separate individual system, has a developed system of perception and processing of information: the second signal system, abstract thinking with the help of concepts, self-awareness, and language. Man can realize the existence of systems, including himself and their development in the past. A person can predict the development of systems and the position of himself in the future. Thanks to the language system, each word is a symbol of a concrete or abstract system. With the help of language, people have the opportunity to transmit, receive, process and store information in the form of entire models of systems. Consciousness with the help of thoughts is engaged in modeling real-world systems, i.e. information processing at the level of system models.

Thoughts and ideas as an objective reality depend on the subject who receives the information, on his prior awareness, education, inclinations and moods, goals and so on. The received information is compared with previous models – "picture of the world" before it will be remembered. Thoughts and consciousness cannot be considered only a reflection of the real world. It is more accurate to call it modeling.

Any real system has infinite variety, dimension and entropy. Consciousness, both mentally and mathematically, cannot operate with infinitely large quantities. Therefore, it creates simplified models that have entropy of finite magnitude.

In a complex model, entropy must be compensated by negentropy – our knowledge and scientific data. That part of entropy that is outside the model of our knowledge and consciousness cannot be compensated by knowledge, but only by faith. Our faith should be as close as possible to real assumptions. Compensation of entropy completely to zero is impossible. In order to overcome the uncertainties of dimension, nature has developed an effective mechanism of the subconscious for humans and animals.

According to Leave E.H. the subconscious is a kind of negentropy. But unlike consciousness, it is not based on specific knowledge, but on previous experience, genetic information of previous generations, feelings, emotions, forgotten, but stored in the depths of the brain information. The experience of the past organism, both positive and negative, is also preserved in the form of changes in the structure of germ, nerve and brain cells.

Part of the hidden information is expressed in the form of instincts, reflexes, and inclinations. The subconscious is also a model, but qualitative and probabilistic. Despite the lack of clear algorithms, models of the subconscious work on the principle of analog and expert systems. They are able to store and process a huge amount of informal information. The subconscious makes it possible to make decisions in the face of a large shortage of time and / or information.

Following the scientific provisions of the work of Leve E.H., by collective system we mean any group of people who have the characteristics of the system, such as the state, family, various organizations, religious and educational societies, and so on. Collectives of people are more complex systems than the sum of individuals. Human consciousness cannot develop in isolation from others.

As a result, we can talk about the collective mind of groups, communities of people, organizations, nation, state, trade unions, and scientific councils and so on. The collective mind is not just the sum of the minds of individuals. When interacting, individual minds can be amplified or suppressed in the struggle. As a result, there is a collective consciousness. In life, this is expressed, for example, in the form of a collective spirit or traditions of scientific and economic organizations, enterprises, sports teams, educational institutions. The collective consciousness cannot be identified with the collective itself. The collective is the primary reality, the consciousness is virtual.

The most common models in the collective consciousness are different theoretical foundations and views on the development of society, state, culture, economy, science, philosophy, and aesthetics.

Model thoughts contain both subconscious and intellectual components, but consciousness also contains elements of faith. Faith "explains" that part of reality that is not taken into account when compiling models. The method of creating imaginary, scientific and intuitive models opens wide opportunities for the study of the real world, to elucidate significant and insignificant factors.

Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text. Paragraph text.

3. Ordinary models of the subject-thinker. Perception and processing of information by a person

As we can see, the process of thinking is a manipulation of a system of models (images) of different types and purposes. Thinking - as an information process - should be based on certain material or virtual media. For the functioning of thinking requires a material or virtual model of the thinking subject. We will use, developed by authors,functionally and deductively complete hierarchical system of abstract information machines, which includes information machines: copying, functional transformation, memory, control, automaton (Turing machine), materializer (processor-designer), processor-thinker.

From a functionally complete hierarchical set of abstract information machines, you can build an information machine of any level, except transcendent, and of any complexity. In [13] it was proved that a hierarchical set of abstract information machines is equivalent to the basis of theoretical semiotics. From the latter, a model of the thinking subject GN Zvereva, which is shown in Fig.1 [14].

A person is a source of words, messages or a receiver of speech, oral or written. The language environment is a finite set of subjects - native speakers and a finite set of communication channels between subjects, which can be transmitted sign names, ie tangible media: signals, texts, images and more. “Language subjects consist of sign processors necessary for the generation, perception, transformation, storage in the subject's memory of sign structures.

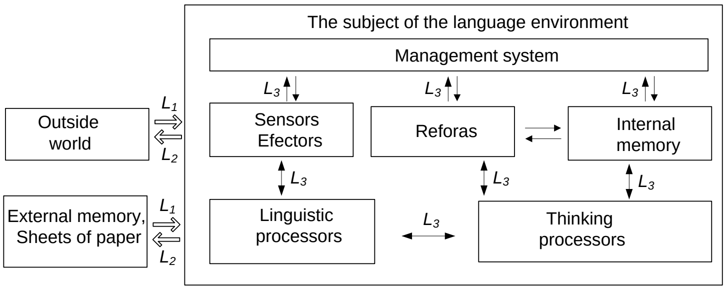

Figure 1: The structure of the objectified subject and linguistic connections

In fig. 1, respectively, L_1 - input, L_2 - output, L_3 - internal language. Any subject of the language environment, establishes language links and communicates with other subjects. Input and output language can be the same for all subjects, ie consist of the same signs and semantics of the language of the subject's linguistic processors. Processor thinkers perform operations on internal signs - the concepts of the subject, included in the internal language, the language of understanding, thinking and emotions.The main types of processors of the subjects of the speech environment (sensor, refor, efor (motor, effector), memory (memory), genor, material processor):

- sensor $A: R_m \to M_s$ performs selective perception of material reality R_m - the physical world and the transformation (reflection) of its properties into signs of virtual reality - a world of signs M_s, information models of physical reality - or identifies the material carriers of message signs;

- refor $B: M_s \to M_s$ performs reforming, transformation of the information world of signs, it is an extremely general functional model of processes of thinking, reasoning, processing of information, data, knowledge, decision-making procedures;

- effector $E : M_s \rightarrow R_m$ it is an arbitrary converter of signs into material objects and actions. Alternative terms: efor, motor;

- accumulator of signs - memory of the subject, memory $G : M_s \rightarrow M_s$ stores knowledge, information in the same form;

- genor $\Gamma \rightarrow M_s$ - internal source (generator) of signs of a certain class, model of generation of signs at modeling of the virtual world of subjects;

- material processor $F_m \wedge R_m \rightarrow R_m$ - a converter of physical reality in which there are no signs, knowledge, information and sign processors».

These types are enough to build language structures, functions, and thus to describe language processes in the language environment.

Sensors (sensors, sense organs, receptors, measuring systems) and effectors (actuators, ideomotor of the body) performs direct and feedback connections of the objectified subject with material reality. The objectified subject is the main object of research of artificial intelligence and theoretical computer science. Sensors, as formal descriptions of the object-transmitter (source) of information are absent in the hierarchical system of abstract information machines. Their equivalent is considered natural and artificial sources of information. And any sensor as an information model can be built from the abstract information machines of this system.

The effector together with the genor and the material processor is the equivalent of the processor-designer (materializer of information that provides the formation, meaning of creation and the whole creation of the receiving object). The role of the reformer (character converter) is performed by abstract information machines of copying, functional transformation (including recursive functions and functionalities) in digital and analog form and automata (in theory - Turing machines) in digital form. In turn, the role of knowledge storage is played by an abstract information machine - memory. So, the model of the thinking subject is an information machine, each of the blocks of which can be built from a hierarchical set of abstract information machines, which is the basis of hierarchical information theory.

But the model of the thinking subject GN The beast can only be part of the heuristic model of the human mind. The mind can act and exist only as a continuous process of perception and processing of information. Intelligence grows in upbringing, domestication, civilization. The process of increasing intelligence over time proceeds successively by leaps and bounds, accumulating the complexity of its structure level by level. When the amount of information at a given level reaches a certain critical value, it is structured, condensed and at the senior level forms the appropriate symbols, concepts, images and relationships. When this level is built, the next higher level begins to be built, and the previous level becomes stable and may continue to have minor changes and improvements. No floor in this building can be missed, as further development becomes impossible. V.M. Lachinov, A.A. Polyakov invented a generalized functional structure of an intelligent control system. The authors completed this structure and supplemented it with a contour of information security (Fig. 2) [15].

The intelligent control system has a system of input and evaluation of information flows for the perception of external control messages and messages from the outside world. The initial flow of information should be considered the final state of the data links that are established in the intelligent database after all the structural agreements and transformations.

The intelligent control and security system must consist of at least three dual intelligent bases that correspond to the controlling entity, the outside world and the object.

In addition, it has subsystems that receive and control information flows from the controlling entity and the outside world, as well as a subsystem for security and internal management. Receiving information flows from the outside world, the corresponding subsystem provides syntactic and semantic control, as well as identification of objects of the outside world. On the basis of these information flows, structures are formed in the intellectual database, which correspond to the knowledge, "images" of the external world and which are used further in the control circuit to compensate for the influences of the external world.

Dual intellectual bases are divided into the left half, where knowledge is accumulated and adjusted, and the right half, where previously accumulated knowledge (images) is stored and reactions to management and influences of the outside world are made using the logic of interaction (Fig. 2 does not show). The logic of interaction is constructed as follows. Intellectual base (IB) "Subject", receiving information from an external management entity immediately rebuilds all its connections. Next, in the right half of the IB "Subject" is a comparison of the existing and new structure to determine the preservation of security and stability of the system, if it agrees to such management. Similarly, there is a restructuring and control of security and stability in the chain of perception of the management of influence from the outside world.

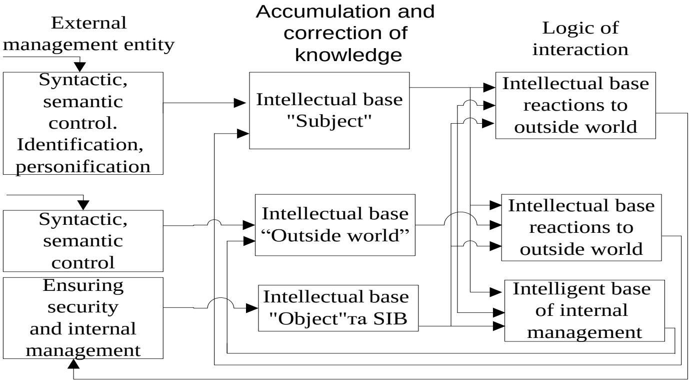
External management entity
Accumulation and correction of knowledge
Logic of interaction
Syntactic, semantic control. Identification, personification
Intellectual base "Subject"
Intellectual base reactions to outside world
Syntactic, semantic control
Intellectual base “Outside world”
Intellectual base reactions to outside world
Ensuring security and internal management
Intellectual base "Object"та SIB
Intelligent base of internal management

Figure 2: Generalized functional structure of intelligent control and security

The intellectual base "Object" includes SIB - security information base, which is used in the cycle of status monitoring and security management.

All three halves of the intellectual databases are brought to a new structure in accordance with the decisions made, which take into account all the structural changes in the hierarchy and correspond to the chosen security and management policy. Eventually, each of the right halves of the intelligent databases informs the left of its agreed state, and the process of generating new information is completed to begin again.

These models do not solve all the problems. Despite optimistic forecasts in recent decades, a model of the human brain has not yet been created. There is a hypothesis that information processing is performed in wave fronts that propagate in neurons. Attempts are also being made to explain the nature of mental activity by quantum effects.

We move on to the final part of our study - making recommendations.

4. Socio-psychological methods of information and cyber security system. Development of recommendation to counter attacks “*myside bias*”

The implementation and function of the cybersecurity system and the provision of social and psychological methods is very important, very important. Here, the subject of scientific advice is individual and collective

The implementation and operation of a system of cybersecurity by socio-psychological methods is as important as it is difficult. Here the subject of scientific research is individual and collective consciousness and individual and collective evidence and subevidence.

4.1. Features of information security systems

Social processes are formed in a complex way, all four consciousnesses act on them. Influences on each consciousness are carried out by various methods, being guided by a matrix of the purposes. Individual and collective consciousness (or mind) is not given to man at birth, but is formed during the growth and life of man. It is changeable and most people are easily affected.

As for the subconscious, it is more stable, exists at the level of instincts, but in certain situations has a decisive influence on human behavior. The subconscious is formed over centuries and millennia. It is as difficult to change it as the mentality.

It turned out that it is quite possible to manipulate people's consciousness and it is possible to form the necessary worldview and individual and collective consciousness. The process of formation of individual and collective consciousness requires: development model, goal of formation (matrix of goals), scenarios of formation procedures and time from several hours for individual elements of influence to change of several generations of people also in separate elements of influence.

Consider the fragments of the information security system of consciousness in terms of socio-psychological security and social engineering. Information security, in addition to its basic importance, acts as an integral part of political, economic, defense, environmental security and more. *Information security means a state* of the information environment (information, information system, information resource) which guarantees the development of this environment and its use in the interests of the individual, society and the state, as well as protection from any threats. For example, it is important for society and the individual to protect their personal data from unlawful processing and accidental loss, destruction, damage due to malicious concealment, failure to provide or untimely submission, as well as protection against providing inaccurate or defamatory information, dignity and business reputation of an individual.

Cybersecurity vulnerabilities can arise as a result of conflicts. Conflict situations arise in wildlife and in human society. The description of the latter is more complicated, because in this case there is a deliberate concealment or distortion of information, special strategies for winning. According to N. Wiener, human language is a joint game of speaker and listener against forces that cause chaos. In fact, the conflicting parties can be not only the forces that cause chaos, but the speaker and the listener. Thus, even in a conversation between people, true information is not always transmitted. In these cases, it is especially important to determine which statement is information and which is noise or misinformation.

From such positions it becomes clear the necessary differences between classical information securities, for example, information in typical computer systems, from information security in a system of consolidated information.

The system of application of consolidated information in activities is generally an open system. It freely exchanges information, energy and matter with the environment and the object of influence. Information security of consolidated information concerns, first of all, the content and essence, semantics of information. Its security must be preventive and continuous. This preserves the traditional requirements for the properties of information: confidentiality, integrity, accessibility and observation. But the protection of the media is not possible at all stages of application of information. The degree of information security changes at different stages of its life cycle. The security system cannot be separated from the process of consolidation and application of information, but must be organically woven into these processes. The security system cannot be of a boundary nature and be an external subsystem relative to the consolidation system. Information security should be formed simultaneously with the formation of goals, essence (semantics) of information. Thus, information security is one of the integral and necessary technological processes of collecting, analyzing, consolidating and applying information.

4.2. Infra-systemic means and self-protection against cognitive distortion

Man is a complex, multi-criteria system. Although it has a number of mechanisms to increase its reliability, it may not always make optimal, often unpredictable decisions and actions. The reason for this is the lack of self-criticism. She usually thinks she knows if not everything, then enough, to make decisions about managing complex systems, such as herself or people's organizations. In fact, these systems have much more entropy than humans have non-entropy on the subject. The result is uncontrollability, unpredictability of system behavior and failure to achieve the goal. A person usually does not admit his mistakes, shifts the blame on others. Unconscious lack of information creates an explosion of emotions, feelings, worries, stress in people, who greatly prevents them from effectively processing information and objectively assess all possible alternatives in the selection and management.

In a state of stress, information processing may stop altogether or, conversely, increase. The emotional state has a lot of options, respectively, and subconscious methods of information processing: fear, anger, enmity, friendship, joy, sadness, and so on. Info flows are especially sharply affected by competition, the struggle for existence, conflict situations. In these cases, they try not only to pass on as little information as possible to the competitor, but even to pass on false information or misinformation. Close to this, there are cases when masking is allowed and even encouraged: sending signals with the conscious purpose of hiding the real intentions of their sender [11].

Here we will understand the peculiarities of protecting the consciousness of the elite and educated people – intellectuals.

Definition Cognitive distortion The "***myside bias***" is a cognitive distortion that forces us to remain true to our own worldviews and those of our group, ignoring evidence that contradicts our views [10].

In many other cognitive distortions, there is an inverse relationship with the level of intelligence – the smarter a person, the less he is exposed to them. But in this case with ***myside bias*** experiments show that everyone is equally exposed to it. This is due to a serious reason, because there is a very reasonable mechanism behind it.

Belief is a kind of generalization, once recorded in our consciousness and subconscious, on which we rely without thinking and without checking its adequacy for this context. Our brain automatically outputs these generalizations to receive some stimulus to simplify our decision-making process. Belief is an illusion of the mind, created once and by someone before, which is perceived as true. This is information that is embedded in the subconscious, which can be trusted, used as a basis for decision making. All beliefs are the fruits of upbringing, which have become entrenched in rigid linguistic forms and now govern thinking and behavior.

Beliefs are fixed in the head on the basis of:

- statements received from elders in childhood and which have received the status of truth;
- own experience, when repeating several similar situations;
- generalization of experience of authoritative and significant for us people;
- and negative thinking and appropriate conclusions about life.

We should evaluate the new information in accordance with the sound position we have. In other words, we need to be skeptical of everything "revolutionary." But you should know that there are views that we have developed through analysis, and there are those that we just want to believe. Political views are rather the latter. We do not so much choose them consciously as we receive in the form of "memes" that infect our consciousness and that comfortably fall on our temperament and character.

And then the ***myside bias*** mechanism starts working, which makes the system of views self-supported, cutting off all inconvenient data. So people are convinced that they have chosen and thought through their position, although in reality it is more of a coincidence, which is disguised as distortion.

This distortion is most dangerous among intellectual elites because they are convinced that they are less prone to distortions than mere mortals. For most distortions, this is true, but not for ***myside bias*** – on the contrary, it makes intellectuals the most blind to this distortion. In the intellectual sphere, critical thinking, working with evidence, discussions, etc. are first needed. And only then, we need identity politics, ideological wars and so on.

It must be understood that belief is a conditioned reflex of the mind, a habit, a stereotypical reaction of understanding, an explanation of the situation when a certain stimulus appears. You can work with conditioned reflexes. They can be installed and removed at will. To counteract the automatic reaction and conditioned reflexes, it is recommended to first ask yourself the following questions:

- How did I know this was really true?
- Are there any examples that contradict this belief?
- Why did I believe it?
- What good is this belief to me? What does it protect me from?

There were ancient beliefs that neither education nor social status alone could guarantee you a deeper understanding of the world around you. This can only give a systematic and persistent work to develop certain qualities (as previously said – "virtues"). Such, as a critical attitude towards yourself and your views. Only this will help us not to get stuck in the "trap of distortion."

4.3. Outside system methods and means of protection against social engineering

The term "system" here means a person. Externally, systemic means and measures of protection must be organically combined and function together with non-systemic measures and means of protection of consciousness. This creates a comprehensive system of protection against social engineering (CSPSI). We will form the following recommendations and substantiate them.

1. Man, team, society are fundamentally open systems. The goals of information security in open systems can be set as follows. In principle, open systems must constantly interact with the outside world. Closing the system, limiting its connections reduces its ability to develop and function and can lead to degradation. The information security system must ensure a certain balance between a certain degree of secrecy and the preservation of opportunities for adaptation and development.

2. Modern society is increasingly beginning to satisfy the laws of development of technical systems, not the development of society, where each person is a conditional technical unit of such a system. For example, the rhythm of oscillations of such units practically coincides with the frequency of the entire state technical system. This allows to integrate into CSPSI, first of all, a certain part of the mechanisms of information security of information resources.

3. Security mechanisms, as well as cybersecurity systems must be adaptable to dynamically changing information flows.

4. The systemic properties of self-preservation, self-organization, self-development and intelligence in terms of open system cybersecurity lead to the requirements of constant control, observation of all systems, phenomena, processes or objects.

5. Information flows between subsystems for cybersecurity and management must be controlled.

6. The tasks of the cybersecurity system can be ranked in the following order: to ensure stability and behavioral (target) aspects of the system; compensate for accidental influences that disturb the system; to reach a state in which accidental influences are compensated, external influences which do not correspond to target functioning of system are blocked.

7. Future security systems should not only and not so much limit users' access to programs and data, but define and delegate their authority in corporate problem solving, detect abnormal use of resources, predict emergencies and eliminate their consequences, flexibly adapting the structure to failures, partial loss or prolonged blocking of resources.

The functional completeness of these recommendations remains unproven.

5. Conclusions

To solve the tasks, the characteristics and features of individual and collective consciousness and the human subconscious as objects of cyber defense are considered; developed, by refining existing models of the thinking machine and intelligent control. A well-founded explanation of the phenomenon of significant vulnerability of the consciousness of the highly educated part of the technical intelligentsia from myside bias is given. Such reasons are the disregard for evidence that contradicts our views, typical of a group of highly educated technical intelligentsia.

Recommendations for counteracting social engineering attacks have been developed, in particular: general system recommendations for the system of protection against social engineering attacks; methods of self-defense against the attack of cognitive distortion "myside bias"; recommendations on non-system methods and means of protection against social engineering.

Due to the high complexity, some of our models of reality are not based on knowledge, but on faith. The rest of the models can be based on the subconscious. Collective consciousness has certain vulnerabilities due to conflicts. Protection against the trap of distortion is a critical attitude towards yourself and your views.

The direction of further work is to create a functionally and deductively complete list of protection mechanisms against social engineering as part of a comprehensive protection system.

6. Acknowledgements

We are grateful to colleagues who always support us and are ready to help. Thanks to the reviewers for carefully reading the work and constructive comments.

7. References

[1] V.L.Buryachok, V.B.Tolubko, V.O. Khoroshko, S.V Tolyupa, Informatsiyna ta kiberbezpeka: sotsiotekhnichnyy aspekt: pidruchnyk; za zah. red. d-ra tekhn. nauk, prof. V. B. Tolubka. K.: DUT, 2015. 288 s.

[2] Alexander Wentland, Nina Klimburg, Hacking Humans? *Social Engineering and the Construction of the “Deficient User” in*

Cybersecurity Discourses. Feb., 2021. URL: https://journals.sagepub.com/doi/full/10.1177/0162243921992844.

[3] Zuoguang Wang, Hongsong Zhu, Peipei Liu and Limin Sun, Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples. *Cybersecurity*. Apr. 2021. 20 p. URL: https://arxiv.org/ftp/arxiv/papers/2106/2106.01157.pdf.

[4] Amy Hetro Wadho, An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behayvior Reports*. Vol. 4. 2021. 23 p. URL:https://www.sciencedirect.com/science/article/pii/S2451958821000749.

[5] Majid H. Alsulami, Fawaz D. Alharbi and etc., Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information*. 2021. URL: https://www.mdpi.com/journal/information.

[6] Vyacheslav Zolotareva, Anastasiya Arkhipovab, Nikolay Parotkina, Anna Lvovac, *Strategies* of *Social Engineering Attacks* on *Information. Resources* of *Gamified Online Education Projects*. *SLET-2020: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education,* November 12-13, 2020, Stavropol, Russia. URL: http://ceur-ws.org/Vol-2861/paper_45.pdf.

[7] Hussain Aldawood, Geoffrey Skinner, Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *International Journal of Security*, Volume (10) : Issue (1) : 2019. 15 p. URL: https://f.hubspotusercontent30.net/hubfs/8156085/WhitePaper%20-%20IJS%20-%20Contemporary%20Cyber%20Security%20Social%20Engineering%20Solutions%5B1%5D.pdf.

[8] Sotsialʹna inzheneriya (systemnyy analiz): navch. posib. [V.M.Petryk, V.I.Kurhanevych, V.H.Kononovych ta in.] / za zah. Red. V.I.Kurhanevycha ta V.M.Petryka. K., 2019. 200 s.

[9] S.P. Rastorguyev, Informatsionnaya voyna. M: Radio i svyaz', 1999. 416 s.

[10] Mikhail Pozharskiy. Lovushka iskazheniy: Naiboleye opasno eto sredi intellektual'nykh elit // Internet-gazeta Svobodnoy Rossii. Url: http://www.kasparov.ru/material.php?id=5F8548820D729

[11] E.Kh. Liyv, Infodinamika, Obobshchonnaya entropiya i negentropiya, Tallinn, 1998.

[12] V.G.Kononovich, I.V Kononovich,. Razdel 20. Osnovy modelirovaniya sistemy kiberbezopasnosti informatsionnogo proizvodstva pri upravlenii massovym soznaniyem, Informatsionnyye tekhnologii v upravlenii, obrazovanii, nauke i promyshlennosti : monografiya / pod red. V. S. Ponomarenko. KH. : Izdatel' Rozhko S. G., 2016. (566 s.) S. 314 - 328.

[13] Kononovych V.H., Kononovych I.V. Infodynamika protsesiv informatsiynoyi vzayemodiyi fizychnoyi ta virtualʹnoyi realʹnosti / *Perspective trajectory of scientific research in technical sciences* : Collective monograph. Riga, Latvia : “Baltija Publishing”, 2021 (644 p.). C. 211 – 234.

[14] Zverev G.N. Metainformatika, iskusstvennyy intellekt i osnovaniya yazyka nauki. Intellektual'nyye sistemy upravleniya. Pod red. akad. RAN S.N. Vasil'yeva. M.: Mashinostroyeniye, 2010. S. 7–16.

[15] Kononovych V.H., Kononovych I.V, Tardaskina T.M. Osnovni pryntsypy informatsiynoyi bezpeky vidkrytykh system. Chastyna 2. Vlastyvosti vidkrytykh system ta vymohy do intelektualʹnoho upravlinnya // Naukovo-tekhnichnyy zbirnyk “Pravove, normatyvne ta metrolohichne zabezpechennya systemy zakhystu informatsiyi v Ukrayini”, – vyp. 2(13), – K.: – 2006. – S. 46 - 57.

[16] O.L. Figovskiy, O.G. Penskiy, Novyye zakony razvitiya obshchestva i budushcheye chelovechestva. 5 c. URL: http://spkurdyumov.ru/future/novye-zakony-razvitiya-obshhestva-i-budushhee-chelovechestva.