International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Conceptual Aspects of Cyber Security

Diyorbek Jo'raev

Tashkent State Information technologies University, Uzbekistan

DOI: https://doi.org/10.55248/gengpi.2023.4112

ABSTRACT:

A significant increase in incidents that occur in the information sphere has led to the need for a systematic analysis of the sources of threats. This requires agreed upon concepts among specialists, the key of which is cybersecurity . It is interpreted ambiguously by many experts. The article proposes an approach to the consideration of the concept of cyberspace and cybersecurity .

Keywords: Information Security, Cybersecurity , Cyberspace, Cybercrime

Currently, there is a sharp increase in information security incidents that are widespread and threatening. Many of these attacks target a wide range of private, corporate, and government interests. The main threat development trends are as follows:

- an increase in the number of attacks, many of which lead to large losses;
- an increase in the complexity of attacks, which may include several stages and apply special methods of protection against possible countermeasures;
- the impact on almost all electronic (digital) devices, among which mobile devices have recently become increasingly important, and they are most susceptible to information security risks;
- Increasingly frequent cases of attacks on the information infrastructure of large corporations, major industrial facilities and even government agencies;
- the use by the most developed countries in the field of computer technology of means and methods of cyber attacks on other states.

This is confirmed by almost daily news reports that report new attacks by criminals in the information sphere. The number of malicious objects that are detected on the network every year is in the billions, and they are distributed to more than 100 million Internet addresses [1, 2]. Every year this number increases by 40% [3]. Attacks in the information space cause damage, which is estimated at 100 billion dollars [4]. According to Alexei Moshkov, head of the Bureau of Special Technical Measures of the Ministry of Internal Affairs of Russia, every second 12 people on Earth become victims of cybercriminals . Only in Russia it was possible to prevent the theft of about 1 billion rubles from the bank accounts of citizens [5]. Of particular danger are threats to mobile devices that have rarely been attacked before. In one year, the number of Android Trojans increased almost 30 times [3].

Extremely complex attack elements have appeared, aimed at worsening the operation of industrial facilities. This is the 2009-detected Stuxnet worm , developed this year by Duqu and Flame , the latter of which has a very complex architecture. It became known about the involvement of American intelligence specialists in the creation of these complex malicious programs. State structures are financing attacks in the field of cyberspace [6]. Numerous attacks on major US banks have been recorded. These attacks have been able to break advanced defense systems and threaten the nation's infrastructure. Presumably, attacks are most often organized from China [7]. At the beginning of the year, a series of attacks were carried out on the largest US media [8], which made the US government once again seriously think about strengthening cybersecurity in the country [9]. In 2013, Kaspersky Lab published information about a completely new phenomenon in the field of computer attacks. Spy network "Red October" (RedOctober)", which has been stealing state secrets for five years. This is the most complex set of malicious programs, about 1000 malicious files belonging to 30 different groups of modules [10]. Similar methods are already actively used for mobile devices on the Android platform [11].

At the end of 2012, American and Chinese government agencies publicly expressed their suspicions of creating equipment with undocumented capabilities, through which networks of another country were attacked from one state. The products of Huawei and ZTE from the Chinese side and Cisco from the American side turned out to be under suspicion [12]. Edward Snowden 's statements confirm the active participation of government agencies in developed countries in collecting information about citizens, officials, corporations and other seemingly public information that can be aggregated to achieve a cumulative effect and obtain classified information. In order to manipulate the public opinion of the masses of people, special methods of social engineering are actively used, largely based on means of communication via the Internet. Thus, there are a number of problems in the field of information security that cannot be fully resolved by traditional means and which should be paid attention to by society and government agencies.

Large-scale violations affecting all aspects of society, based on the latest methods of attacking computer networks, as well as public consciousness control, require a systematic approach to creating an integrated security system that can withstand these threats. A general analysis of the problematics of protection against similar, emerging and continuing to develop threats can be denoted by the concept of cybersecurity . The issues of ensuring cybersecurity were analyzed in [13] and the need for large-scale measures on the part of the state to ensure security in the field of information and telecommunication technologies (hereinafter referred to as ICT) was shown. We are talking about the coordination of efforts in this direction of state bodies, business and society as a whole. Such a complex task should be solved on the basis of a clearly developed position, an unambiguous understanding of what is meant by cybersecurity . In [14], approaches to the development of terminology in this area are considered. Obviously, cybersecurity should be aimed at providing protection in cyberspace. Therefore, the concept of cyberspace is the main one for analyzing cybersecurity problems. To understand its content, it is advisable to rely on the term cybernetics. Cybernetics (from the Greek “art of management”) is the science of management, communication and information processing.

An abstract cybernetic system is a set of interconnected objects, called system elements, capable of receiving, storing and processing information, as well as exchanging information. That is, the subject area of cybernetics includes all modern information and telecommunication technologies. It is important that within the framework of the cybernetic approach, the elements of the system are considered as continuously interacting with each other and people are included as important constituent elements in cyberspace - active participants in information exchange and the use of information resources. At the beginning of 2014, the Federation Council proposed for public discussion a draft Concept of the Cybersecurity Strategy of the Russian Federation (hereinafter referred to as the Concept). It is designed to determine the direction of the state's efforts in relation to new threats that arise in the modern information world [15]. The concept of cybersecurity is very multifaceted and therefore not easy and difficult to formalize. There are a lot of different ideas and views here. Information security specialists and simply interested users, in particular, those who left comments on the Concept, express very conflicting views on this issue. An analysis of the comments shows that one of the main problems in the development of such documents is the difficulty in understanding the term cyberspace and the related concept of cybersecurity .

Cyberspace in the draft Concept is defined as follows: “Cyberspace is a sphere of activity in the information space, formed by a combination of communication channels of the Internet and other telecommunication networks, the technological infrastructure that ensures their functioning, and any forms of human activity carried out through their use (individuals, organizations, states) ". In principle, such a definition to some extent interprets certain aspects of this important concept, but the lack of further detailed explanations leads to an inaccurate understanding of it.

The vast majority of experts who left their comments on the draft Concept believe that the definition deals exclusively with the technological component of the information field, that is, with computer and telecommunications infrastructure. The issue of activity based on this infrastructure and any kind of human activity that is carried out through technology is completely overlooked. And this is directly stated in the definition. For a document of such importance, this is unacceptable and indicates the need for further methodological work to define cybersecurity as a characteristic of cyberspace. The definition given in the concept has much in common with the position of the international standard ISO/IEC 27032:2012 Cybersecurity Guidelines (ISO/IEC 27032:2012 Informationtechnology - Securitytechniques - guidelinesforcybersecurity).

Cyberspace is a complex environment that does not exist in any physical form, resulting from the interaction of people, software, Internet services through technological devices and network connections. In a policy article on cybersecurity , UK specialists define this concept as any activity in a networked, digital form, adding after that that this also includes information content and actions carried out through digital networks. (Klimburg A. et al. National cyber security framework manual //NATO CCD COE Publications (December 2012). – 2012. http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-nato-manualch-1 .pdf).

With all the variety of these definitions, it can be noted that with a clear indication of the connection between cyberspace and ICT infrastructure, the focus is not on technologies, but on the activities of people who use these technologies. It is important that the main content of cyberspace lies in the activities of users of digital information resources and ICT infrastructure. Cyberspace can be viewed as a triad, which includes three main components. Information in its digital representation: static (files recorded on data carriers) and dynamic (packets, streams, commands, requests, etc. transmitted over various networks, processed in automated systems and presented on display devices in graphic or text form). Technical infrastructure, ICT, software, with the help of which the implementation of the main actions with information is carried out: collection, processing, storage and transmission. Such means include the infrastructure of the Internet and network interconnections, computers, all kinds of gadgets, etc.

Information interaction of subjects using information received (transmitted) and processed through the technical infrastructure. This refers to all types of activities of users or participants in cyberspace that they carry out using information resources, the flows and storages of which are located on the technical infrastructure.

All these components together form an entity that can be called cyberspace. The following main properties can be distinguished. First. Cyberspace is defined on a variety of digital devices and systems based on them, which operate with information or, in many respects, with its help. It is important that we mean not separate systems, but their combination, when there are a lot of such devices (systems). That is, in general, a significant decrease in the number of functioning devices (systems) in cyberspace or a violation of their normal operation is a threat to cyberspace. But we are talking not just about individual devices (systems), but about a large number of such objects and the ability to operate them with information (provide services) with a given quality, that is, to perform actions that are usually associated with information technology. This is where the second property comes from. Active handling of information and preservation of this information of its main properties: integrity, accessibility, confidentiality and others defined in modern standards. Unlike information security, we are not talking about information in general, but about the information that circulates in cyberspace and is an important part of its content. Thus, the disruption of the operation of a separate computer connected to cyberspace or the loss of information that it contains, or the violation of its properties, which are certainly important for the user of this computer, can hardly be considered a threat to cybersecurity . Third. The presence of “respectable” connections, connections that form the basis of cyberspace, and without which it would hardly make sense to consider the field of digital devices (systems) as some new entity. This refers to the ability of cyberspace to transmit, receive and process information while maintaining its essential properties for the purposes of application. Fourth. Actually the concept of cyber -. It refers to management. Management in this case does not imply the presence of straightforward commands that are directly executed by all agents (participants) of cyberspace, but the formation and transmission of such signals that can give the area of cyberspace under consideration a certain “reasonable” behavior and resistance to emerging threats. Management methods have a direct impact on the structure of cyberspace.

Here it is important to take into account the management of the technical basis of cyberspace and the purely physical links between individual nodes or even areas of cyberspace. But the decisive role is played by the management of cyberspace participants: users and their groups. Management refers to a set of efforts aimed at improving the skills of participants, stimulating actions that are favorable for the development of cyberspace and suppressing or outright prohibiting malicious actions.

The management of cyberspace subjects plays a decisive role in the emergence, existence and maintenance of the main properties of this formation. These properties, namely the multiplicity of elements that make up cyberspace, the abundance of interconnections between them, the possibility of using special techniques to control the actions of these elements, determine the development of the threats mentioned above. The unusually high and ever-increasing intensity of attacks comes from the vast scale of cyberspace, all kinds of and diverse connections between them. Sophisticated attacks, which have a complex structure, rely on the possibility of various directions for the propagation of information and signals. The use of social engineering methods makes it possible to find the most productive methods of organizing attacks. Increasingly dangerous and complex threats can develop in cyberspace. They use the features of its construction to achieve maximum effect. But the same features, stemming from the many interrelations between actors in cyberspace, can be an important factor in improving the effectiveness of systems that provide protection against such threats [16]. To do this, it is necessary to coordinate the efforts of all interested participants, to create mechanisms that contribute to the best distribution of their efforts. It is necessary to correctly identify emerging and predicted hazards and reasonably choose rational protective measures.

Cybersecurity aims to address these issues and ensure the normal functioning of cyberspace, protecting it from emerging threats in an effective manner. It is important to correctly formulate the concept of cybersecurity , so that the main goals of the work of services and means of protecting cyberspace from emerging threats are precisely defined. However, the concept contains a formulation that cannot meet these requirements.

The draft Concept states the following: “ cybersecurity is a set of conditions under which all components of cyberspace are protected from the maximum possible number of threats and impacts with undesirable consequences.”

Cybersecurity cannot be aimed at protecting against the maximum number of threats. It is necessary to provide the most favorable environment for the work of users and all systems in cyberspace. The formulation specified in the Concept implicitly calls for the development and identification of more and more new threats, creating new means and methods of protection against them. The share of resources needed to provide protection, with this approach, will steadily increase, and the stable operation of cyberspace may even worsen. Therefore, in the definition of cybersecurity , the main emphasis and target setting should be made on maintaining a favorable state of cyberspace, and not on the number of threats. If we can defend against an unimaginably large number of threats, but the health of cyberspace is broken, then this is worse than defending against two dozen threats and at the same time maintain an acceptable level of health.

Cybersecurity , just like cyberspace, can be described by a triad of its constituent entities defined on the components of cyberspace: information resources, computer and network architecture (infrastructure) and ways of user interaction. Cybersecurity no longer covers only information as an object of protection, not only technical means that determine the possibilities for the functioning of information, but the protection of the ways of functioning of a new entity - cyberspace. The activity of people, which is carried out with the help of information disseminated through the technical infrastructure of ICT, is protected.

When ensuring cybersecurity , it is important to take into account these features of cyberspace and its most important aspect - the existence of relationships between participants (users), which leads to the possibility of a synergistic effect. The draft Concept indicates the need to conduct scientific research in the field of cybersecurity , in particular, the implementation of scientific and technical programs and research in accordance with the "Priority areas of scientific research in the field of information security of the Russian Federation", approved by the Security Council of the Russian Federation. But this is only a general statement, referring to a list of more than 100 areas, among which it is necessary to highlight the most significant from the point of view of cybersecurity . It is in these directions that the main efforts should be concentrated. Proposals for such works are given in the article [17]. In addition, the subject of advanced research should be supplemented with directions that follow from the basic properties of cyberspace. It is necessary to study in detail and carefully the main properties of cyberspace, the dynamics of its development on various time scales from instantaneous to long-term, and methods for managing this dynamics.

It is important to justify approaches to the definition of cybersecurity indicators , develop models for their evaluation, and develop ways to justify the criteria. It is impossible to build an effective cybersecurity system without conducting a system analysis and obtaining assessments of the application of certain measures . It seems appropriate to include the following areas in the complex of research in the field of cybersecurity :

1. Development of a unified terminology for cyberspace and cybersecurity , harmonized with the existing terminology in the field of information security.

2. Development of a comprehensive system of indicators covering all aspects of the functioning of cyberspace and ensuring its protection from possible threats.

3. Development of models of cyberspace itself and the main factors influencing its functioning. Of course, a carefully thought-out threat model is needed. One of the most important areas is the creation of mathematical models that allow obtaining numerical characteristics of information security (degrees of threats to information security, analysis of information risks, evaluation of the effectiveness of protection measures).

4. Creation of special methods for ensuring the stability of cyberspace or its areas under the influence of threats. There are several possible topics here: - analysis of the topological structure and development of recommendations for changing it, methods and specific algorithms for their implementation; - new methods of cryptographic protection, based not only on purely computational mechanisms for implementing security, but also on using the advantages of a multi-connected architecture of links and a large number of respectable users; - methods of information security based on social services to counteract cyber attacks using special procedures for analyzing group behavior.

5. Intelligent cyber security methods :

- methods of intellectual identification of users;
- intelligent methods to prevent virus and other attacks;
- intelligent methods for detecting attacks and intrusions;
- methods of situational analysis of the state of information security;
- new methods of cryptographic protection based on neural network technologies.

References

1. http://www.securelist.com/ru/analysis/208050763/ Razvitie_informatsionnykh_ugroz_vo_vtorom _ kvartale_2012_goda.

2. Trustwave 2013-Global-Security-Report

3.ht _p : / / w ww . symantec. com/secur i ty_response /publications/ threatreport.jsp

4. 2012 Norton Cybercrime Report _ _

5. http://mvd.ru/news/item/1033853

6. http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/cyber-attacks.aspx

7. http://www.cybersecurity.ru/crypto/171331.html

8. http://www.politico.com/story/2013/02/washingtoncybersecurity-china-attacks-87087.html

9. http://www.nytimes.com/2013/01/28/us/pentagon-tobeef-up-cybersecurity-force-to-counter-attacks.html

10. http://habrahabr.ru/company/kaspersky/blog/169839/

11. http://www.itsec.ru/newstext.php?news_id=91005

12. http://www.cybersecurity.ru/telecommunication/165487.html

13. Starovojtov AV Kiberbezopasnost ' kakactual'najaproblemasovremennosti (Cybersecurity as an actual modern problem) // Informatizacijaisvjaz ' (Informatization and communication). – 2011. – no. 6. - P. 4-7.

14. Bezkorovajnyj MM, Losev S.A. , TatuzovA.L . Cyberbezopasnost 'v modern mire: terminyicontent (Cybersecurity in the modern world: terms and content) // Informatizacijaisvjaz ' (Informatization and communication) - 2011. - no. 6. - P. 27-32.

15. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73. pdf

16. Bezkorovajnyj MM, TatuzovA.L . Approach to mathmaticheskomumodelirovaniju v oblasticyberbezopasnosti (Approaches to mathematical modeling in sphere of cybersecurity) // Informatizacijaisvjaz ' (Informatization and communication). – 2011. – no. 6. - P. 21-27. 17. Bezkorovajnyj MM, TatuzovA.L . Informationnajabezopasnost ' v sphereobrazovanijainauki (Information security in the sphere of education and science) // Informatizacijaisvjaz ' (Informatization and communication). – 2011. – no. 6 . – P. 34-39.