Modern cybersecurity from the perspective of cognitive modeling

Irina Lapshina[1] *and Andrey Kravets*[2]

[1]*Taganrog Institute named after A. P. Chekhov, branch of RSUE (RINH)*
[2]*Taganrog Institute of Radio Engineering Systems and Control, Southern Federal University*

Abstract: In the article, the authors examine the problem of ensuring cybersecurity in the modern world in terms of the study of social practices. The implemented cyber-attacks are analyzed, and the danger of hacker attacks is shown. With a fair amount of evidence, it can be stated that in the modern world, the risks associated with cyber intrusions can include the loss or disclosure of consumer data, theft or disclosure of intellectual property, as well as the loss of investors as a result of the theft of funds or a decrease in the market value of companies subjected to cyber-attacks. It is concluded that cybersecurity is a constantly evolving landscape, and now there is an urgent need to constantly learn from both our own experience and the experience of other companies countering cyber-attacks effectively, and it is also important that successful interaction with adversaries in cyberspace requires a constant pursuit of a tactical, operational and strategic initiative.

Keywords: cyber wars, cognitive modeling, cyber-attacks, hacker attacks, cyber risks, cyber defense.

Introduction.

At the beginning of our research, we will analyze the practice of "small" wars and armed conflicts that have occurred in the world outside the post-Soviet space, which is quite understandable, given that the past XX century is a century of confrontations at various levels. In our opinion, the central danger in the world community has become the fact that America has entered a permanent "global war on terrorism", which is being waged, in fact, across the globe in the form of a multitude of large and small interventions [1].

It should be noted that the fear of suffering from the actions of terrorists, according to I. N. Titarenko, is experienced by 74% of Russians, and the threat of terrorism itself in the mass consciousness occupies a leading position and outstrips such threats as transport accidents, environmental disasters, poisoning with chemicals in products. Russian citizens consider terrorism and extremism based on Islamic fundamentalism especially dangerous [2, p. 194].

So, the example of a conflict between Sinhalese (Buddhists by religion) and Tamils (Hindus) in Sri Lanka, 1987 in which the Liberation Tigers of Tamil Eelam began to resort to the practice of suicide bombing attacks and, accordingly, special training of kamikaze fanatics was carried out which in turn can be positioned as a variant of the initial level of training a network warrior in terms of the impact on the consciousness of the future suicide bomber.

Next, let's talk about the 1995 armed conflict between two Latin American countries - Peru and Ecuador. The advantage in this armed conflict was that Ecuador was able to organize a fairly successful targeting of its aircraft with the help of a timely deployed ground radar near the border line, while the Peruvian side had no radar coverage in the conflict zone, which can also be described as an element of network-centric warfare. those. wars of a new type. Currently, the main tactical principle of the Russian information war is the concept of "reflexive control". According to Timothy L. Thomas, an analyst at the Center for the Study of Foreign Armed Forces under the US Army and an expert on contemporary Russian military history and theory, reflexive control involves “passing on specially prepared information to the enemy in order to convince him of his own free will to make a decision, beneficial to the initiator of the transfer” [3, p. 15]. This allows us actually to talk about the use of psychological coercive mechanisms that affect the consciousness of the enemy. "While cyber warfare at the military level refers to conflict related to knowledge, network warfare refers to social warfare, most often associated with low-intensity conflicts by non-state actors such as terrorists, drug cartels or black-market dealers of weapons of mass destruction." [4]. Consequently, future wars will be fought over civil and military infrastructure satellite systems, electrical networks, communications and transportation systems, and human-to-people networks. These battlefields – both electronic and human ones - are subject to manipulation by enemy algorithms [5].

Rosa Brooks, American law professor, journalist, author and commentator on the US foreign policy, notes that “... cyber battles will be associated with those who can control the machines of everyday life: the servers that the Pentagon and the New York Stock Exchange rely on, computers that monitor the work of the brakes of our cars, the software that starts our home computers ...” [6].

Methods.

Cognitive modeling methods are used to make cognitive maps. Nowadays, every Internet user needs to watch out for email fraud and phishing. What may appear to be a legitimate site may in fact be a scam. The link may at first glance be from a legitimate seller, but the title may contain, for example, an additional letter. To be safe, you need to go directly to the website of the company from which the email was sent to avoid clicking on malicious links that could lead to accidentally downloading malware or spyware to your computer, tablet or mobile phone.

So, we are talking about the possibility of influence in cyberspace, which is both an environment for conflict and its instrument, and here the issue of power and coercion arises. If classical geopolitics uses the concepts of Sea Power and Land Power, and later there was air domination and domination in space, then recently they started talking about new power or domination in cyberspace (Cyber Power). A significant difference between hot wars and potential cyber wars is that cyberattacks have not yet led to the death or injury of people, therefore, they cannot be classified as military actions due to the absence of physical violence [7].

According to Joseph S. Nye, “Cyber power can be used to produce preferred outcomes in cyberspace, or it can use cyber tools to obtain preferred outcomes in other areas outside of cyberspace” [8]. At the same time, the following should be noted: freedom of action is a characteristic of superiority in cyberspace, so, for example, cyber attacks are supposedly not to be used against exclusively civilian objects. However, this is not quite the case, as social practice shows. We will find the embodiment of this idea in a more or less explicit form in practice, Barton

Gellman and Laura Poitras in the article “British intelligence mining data from nine U.S. Internet companies in a broad secret program” claim that the NSA and the FBI connect directly to the central servers of nine leading US Internet companies, retrieving audio and video chats, photos, emails, documents, and connection logs that allow analysts to track foreign targets. according to a top-secret document obtained by The Washington Post. Also, the US National Security Agency secretly hacked into the main communication channels connecting Yahoo and Google data centers around the world, according to documents obtained from former NSA employee Edward Snowden and interviews with knowledgeable officials [9]. In turn, government requests for obtaining customer data are provided by Microsoft Corporation, this activity is carried out by using modern cloud technologies based on openness and availability. While Microsoft employees say they place great emphasis on respecting and protecting customer privacy, Microsoft recognizes that law enforcement plays a critical role in customer safety. “At the same time, we believe that our customers deserve predictability in how and when the government can access their data, and this should depend on national laws and international human rights standards, and not on the discretion of any company. to determine where the border lies” [10].

Here is an example of a Stuxnet cyber-attack (worm) on an Iranian nuclear power plant. It was the first registered digital weapon to be used to destroy physical resources. Like any other attack, Stuxnet followed the previously described steps and stayed on the network of the object for a year. Stuxnet was originally used to manipulate valves in a nuclear facility, resulting in pressure build-up and damage to several devices in the station. The malware was then modified to attack a larger target - centrifuges. So, as researchers Diogenes Y. and Ozkaya E. note in Cybersecurity: Strategies for Attack and Defense, the Iranian nuclear facility had no chance of defending itself since the attackers had already gained access, increased their privileges, and remained out of sight of security equipment. Another example in modern cyberspace is the data manipulation variant. This is due to the fact that this is already the next stage of cybercrime and it is expected that there will be many more such cases in the near future. It is said that industrial enterprises in the United States are not prepared for such attacks. Cybersecurity experts warn against imminent threats of manipulative attacks on medical, financial and government data [11, p. 96]. At present, the danger of hacker attacks is great, and in this case, the combination of permissiveness with invisibility makes hackers dangerous. Cybersecurity has become an important topic in both the private and public sectors, and for good reason. Law enforcement agencies and financial regulators have publicly stated that cyberattacks are becoming more frequent and sophisticated [12].

Cyber threats are increasingly becoming more vital for financial services institutions and other companies that have been targeted by sophisticated hacker groups. They can safely intercept passwords and data on the network, add bookmarks to programs for subsequent unauthorized access, and attack other nodes on the network. As Erickson D. Hacking points out, viruses and worms cause a lot of troubles and bring big losses to the business, but at the same time they force developers to retaliate to solve the problems that arise. Worms reproduce themselves by exploiting the vulnerabilities of low-quality software. Often, errors go unnoticed for years, and relatively harmless worms, such as CodeRed or Sasser, force developers to fix them [13, p. 350]. Enterprises must therefore conduct regular, comprehensive risk assessments of the cybersecurity threats they face, including external and internal threats and the vulnerabilities of their assets. While there is currently no “one size fits all” option to adequately prepare for the various cyber attacks and what responses might be appropriate, a poorly implemented response to a cyber event can be just as devastating. According to analysts, a poorly thought-out response can be far more damaging than the attack itself. Accordingly, businesses must invest time and resources to ensure that their management has developed a well thought out response plan that is in line with best practices for a company in the same industry.

In other words, before cyber risks can be mitigated, the security team must conduct an in-depth analysis of the vulnerabilities it faces. In an ideal IT environment, the security team can respond to all vulnerabilities if they have sufficient resources and time. However, there are many limiting factors when it comes to the resources available to mitigate risks. Therefore, risk assessment is critical. For example, if cybersecurity risks significantly affect products, services, an organization's relationships with customers or suppliers, or competitive conditions, the organization should disclose those risks. Cybersecurity risks and incidents that represent a significant cost to prevent or respond should be made public.

All this allows researchers to say that a cyber-attack may not have a direct material negative impact on the company, but the fact that the loss of personal and financial data of customers can have devastating consequences for the lives of the company's customers, is undeniable. In such cases, it is wise to give these victims a warning so that they can protect themselves. In addition to the above, it should be said about the following aspect associated with a wide range of problems aimed at solving problems of ensuring cybersecurity by enterprises. For example, Alan Woodward, a cybersecurity expert, and professor at the University of Surrey (England) notes that focusing on educating people in non-technical roles so that they get more prepared in cyberspace security sphere tends to put too much pressure on people [14]. As a result, cybersecurity is a constantly evolving landscape, and today there is an urgent need to constantly learn from both our own experience and the experience of others.

At present, the world and international relations are characterized by many significant processes that are just beginning to be examined by the specialists in the field of social sciences. In general, experts are inclined to believe that the very foundation of cyber troops increases the ability of the armed forces to operate in cyberspace, as well as cyber defense requires "protection forward", participation in real international military operations will be valuable from the standpoint of acquiring the skills of developing cyber tools and cyber troops in general [15, p. 5]. In international relations, the sphere of cyberspace can no longer be considered as something of secondary importance, since in modern combat operations cyber tools are considered vital for the successful fulfillment of numerous tasks and it should be noted that activities in cyberspace over time can undermine the sources of a country's national power. In this connection, there is an urgent need for government networks and the defense industry of states to become increasingly cyber-capable, since the sphere of confrontation is moving from the field of open conflict and violent operations to cyberspace, bypassing the sphere of military conflicts with the use of lethal weapons. Cybersecurity efforts should include, in addition to assessment, prevention, mitigation, resilience and recovery. In today's environment, cyber-attacks are perpetrated by identity thieves, unscrupulous contractors and suppliers, malicious employees, business competitors, potential insider traders and market manipulators, so-called “hacktivists,” terrorists, government-sponsored actors, and others.

Cybercrimes can pose significant risks to the operations of market participants and markets in general. These risks can take the form of denial of service and system disruption, potentially leading to impediments to account access and transactions, as well as disruption of other important functions of the market system. Risks associated with cyber intrusions can also include the loss or disclosure of consumer data, theft or disclosure of intellectual property, and the loss of investors due to theft of funds or a decline in the market value of companies subjected to cyberattacks, among others. Market participants also face regulatory, reputational and litigation risks arising from cyber incidents, as well as the potential for significant remediation costs. Samuel P. Huntington accordingly identifies two major factors that determine the success of a strategic concept: resources, both human and material ones, and an organizational structure that groups the resources allocated by society in a specific way to implement the strategic framework [16].

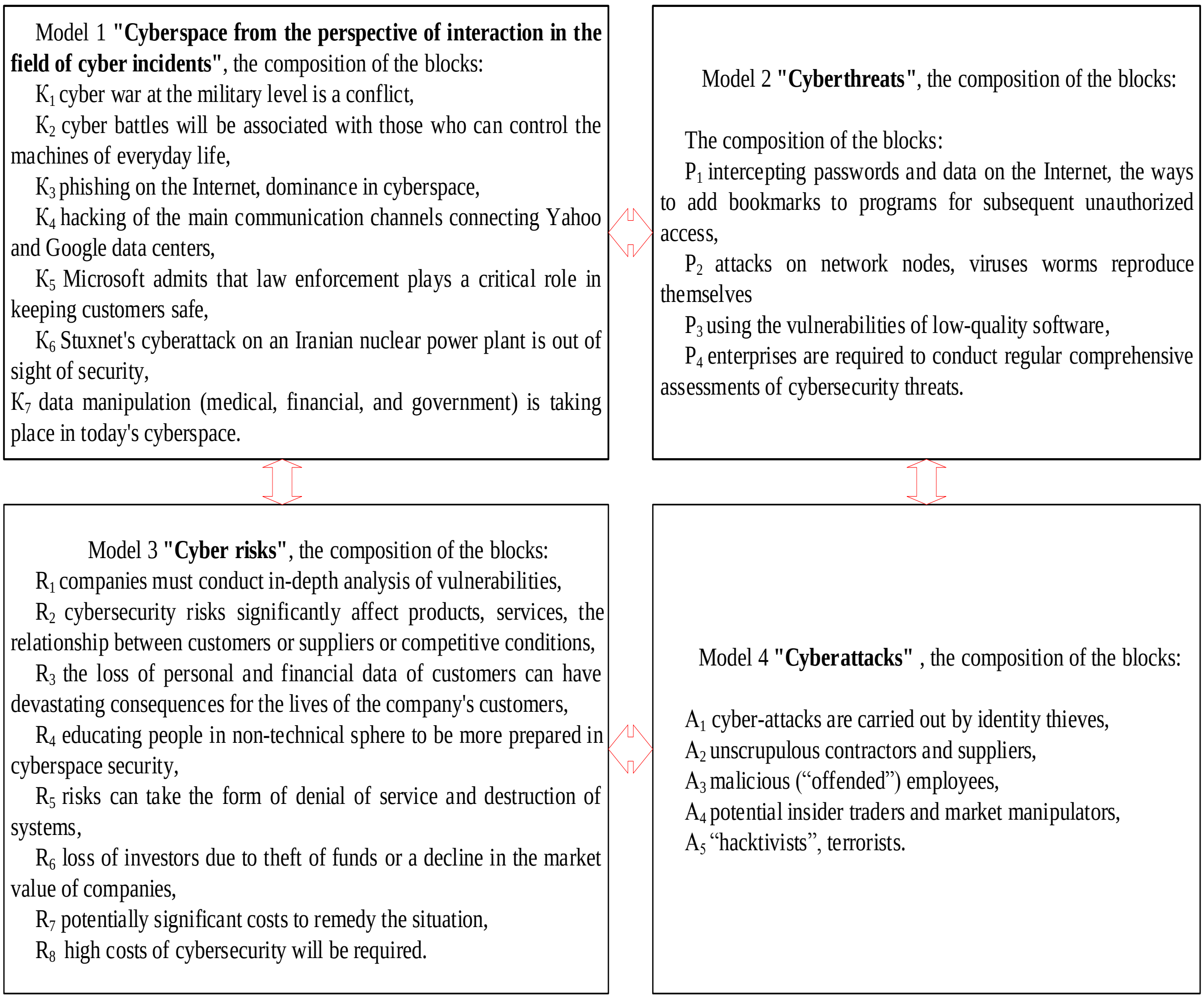
Results.

The composition of the blocks and their interaction in the model "Reflexively controlled cyber wars of modernity" (fig. 1).

Let us examine the blocks of factors, in Model 1 **"Cyberspace from the perspective of interaction in the field of cyber incidents":** $К_1$ cyber war at the military level is a conflict, $К_2$ cyber battles will be associated with those who can control the machines of everyday life, $К_3$ phishing on the Internet, dominance in cyberspace, $К_4$ hacking of the main communication channels connecting Yahoo and Google data centers, $К_5$ Microsoft admits that law enforcement plays a critical role in keeping customers safe, $К_6$ Stuxnet's cyberattack on an Iranian nuclear power plant is out of sight of security, $К_7$ data manipulation (medical, financial, and government) is taking place in today's cyberspace.

Let us highlight the blocks of factors in Model 2 **"Cyber threats":** P_1 intercepting passwords and data on the Internet, the ways to add bookmarks to programs for subsequent unauthorized access, P_2 attacks on network nodes, viruses worms reproduce themselves, P_3 using the vulnerabilities of low-quality software, P_4 enterprises are required to conduct regular comprehensive assessments of cybersecurity threats.

Let us consider the blocks of factors, in Model 3 **"Cyber risks":** R_1 companies must conduct in-depth analysis of vulnerabilities, R_2 cybersecurity risks significantly affect products, services, the relationship between customers or suppliers or competitive conditions, R_3 the loss of personal and financial data of customers can have devastating consequences for the lives of the company's customers, R_4 educating people in non-technical sphere to be more prepared in cyberspace security, R_5 risks can take the form of denial of service and destruction of systems, R_6 loss of investors due to theft of funds or a decline in the market value of companies, R_7 potentially significant costs to remedy the situation, R_8 high costs of cybersecurity will be required.



Model 1 **"Cyberspace from the perspective of interaction in the field of cyber incidents"**, the composition of the blocks:

K_1 cyber war at the military level is a conflict,

K_2 cyber battles will be associated with those who can control the machines of everyday life,

K_3 phishing on the Internet, dominance in cyberspace,

K_4 hacking of the main communication channels connecting Yahoo and Google data centers,

K_5 Microsoft admits that law enforcement plays a critical role in keeping customers safe,

K_6 Stuxnet's cyberattack on an Iranian nuclear power plant is out of sight of security,

K_7 data manipulation (medical, financial, and government) is taking place in today's cyberspace.

Model 2 **"Cyberthreats"**, the composition of the blocks:

The composition of the blocks:

P_1 intercepting passwords and data on the Internet, the ways to add bookmarks to programs for subsequent unauthorized access,

P_2 attacks on network nodes, viruses worms reproduce themselves

P_3 using the vulnerabilities of low-quality software,

P_4 enterprises are required to conduct regular comprehensive assessments of cybersecurity threats.

Model 3 **"Cyber risks"**, the composition of the blocks:

R_1 companies must conduct in-depth analysis of vulnerabilities,

R_2 cybersecurity risks significantly affect products, services, the relationship between customers or suppliers or competitive conditions,

R_3 the loss of personal and financial data of customers can have devastating consequences for the lives of the company's customers,

R_4 educating people in non-technical sphere to be more prepared in cyberspace security,

R_5 risks can take the form of denial of service and destruction of systems,

R_6 loss of investors due to theft of funds or a decline in the market value of companies,

R_7 potentially significant costs to remedy the situation,

R_8 high costs of cybersecurity will be required.

Model 4 **"Cyberattacks"** , the composition of the blocks:

A_1 cyber-attacks are carried out by identity thieves,

A_2 unscrupulous contractors and suppliers,

A_3 malicious (“offended”) employees,

A_4 potential insider traders and market manipulators,

A_5 “hacktivists”, terrorists.

Fig 1. – The composition and interaction of model blocks "Reflexively controlled cyber wars of modernity".

Let us examine the blocks of factors in Model 4 **"Cyber attacks":** A_1 cyber attacks are carried out by identity thieves, A_2 unscrupulous contractors and suppliers, A_3 malicious (“offended”) employees, A_4 potential insider traders and market manipulators, A_5 “hacktivists”, terrorists.

It is known that a cognitive map is a weighted directed graph [17].

$$G = <V, E>,$$

where V – graph nodes:

$$V = \{v_i\}, v \in V, i = \overline{1,k}; \qquad (1)$$

E – edge of a graph:

$$E = \{e_i\}, e \in E, i = \overline{1,k}.$$

L. A. Ginis asserts that the goal of cognitive modeling is to generate and test hypotheses about the functional structure of the observed situation until a functional structure obtained can explain the behavior of the observed situation [18]. Cybersecurity issues have been also analyzed by the authors [19].

In fig. 1-4 solid lines and the symbol "+1.00" denote a positive relationship between the peaks Vi and Vj, that is, an increase (decrease) in the influence of the peak Vi causes an increase (decrease) in the peak Vj, the lines and the symbol "-1.00" mean negative relationship between Vi and Vj, that is, an increase (decrease) in the influence of the top Vi causes a decrease (increase) in the top Vj (fig. 1).

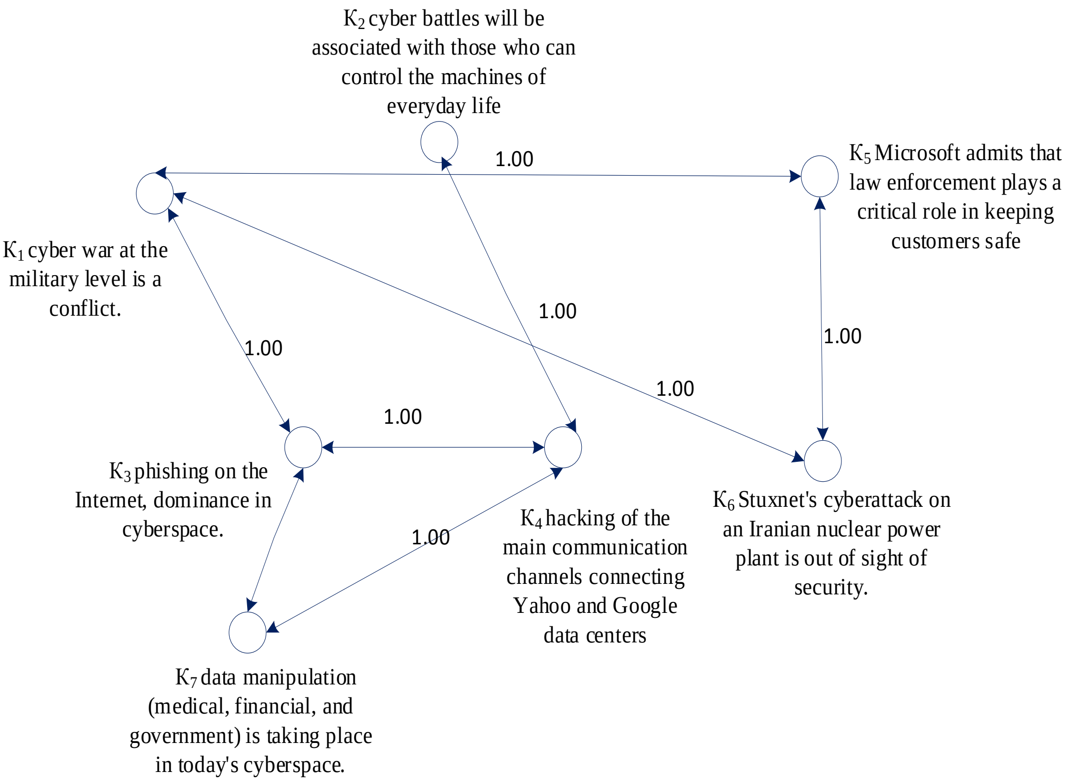

K2 cyber battles will be associated with those who can control the machines of everyday life
K5 Microsoft admits that law enforcement plays a critical role in keeping customers safe
K1 cyber war at the military level is a conflict.
K3 phishing on the Internet, dominance in cyberspace.
K4 hacking of the main communication channels connecting Yahoo and Google data centers
K6 Stuxnet's cyberattack on an Iranian nuclear power plant is out of sight of security.
K7 data manipulation (medical, financial, and government) is taking place in today's cyberspace.
1.00
1.00
1.00
1.00
1.00
1.00
1.00

Fig 2. – The interaction of the blocks in Model 1 "Cyberspace from the

perspective of interaction in the field of cyber incidents".

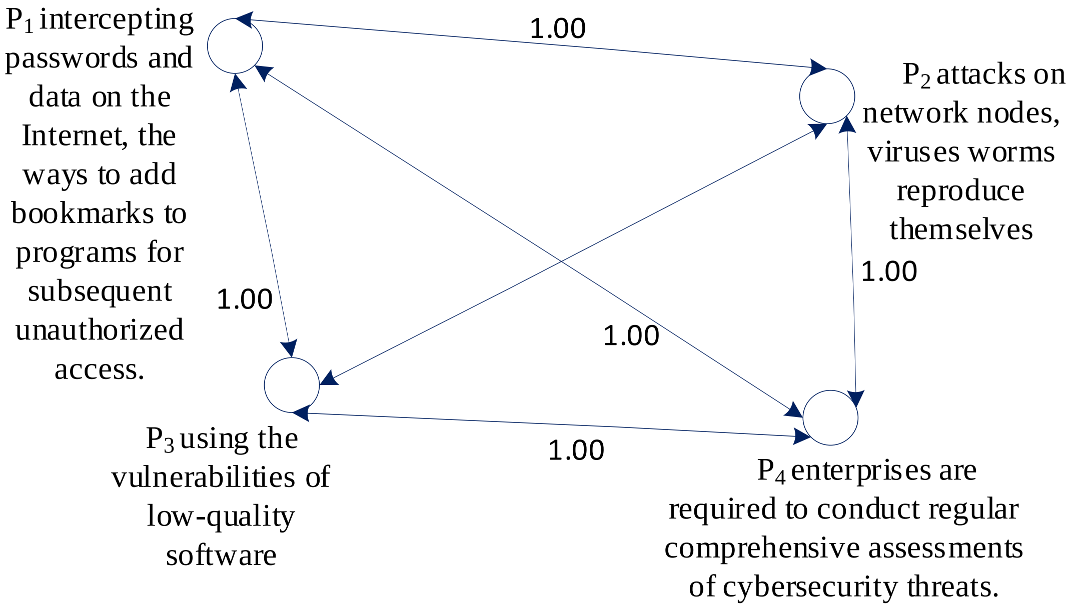

P_1 intercepting passwords and data on the Internet, the ways to add bookmarks to programs for subsequent unauthorized access.
1.00
P_2 attacks on network nodes, viruses worms reproduce themselves
1.00
1.00
1.00
P_3 using the vulnerabilities of low-quality software
1.00
P_4 enterprises are required to conduct regular comprehensive assessments of cybersecurity threats.

Fig 3. – The interaction of the blocks in Model 2 "Cyber threats".

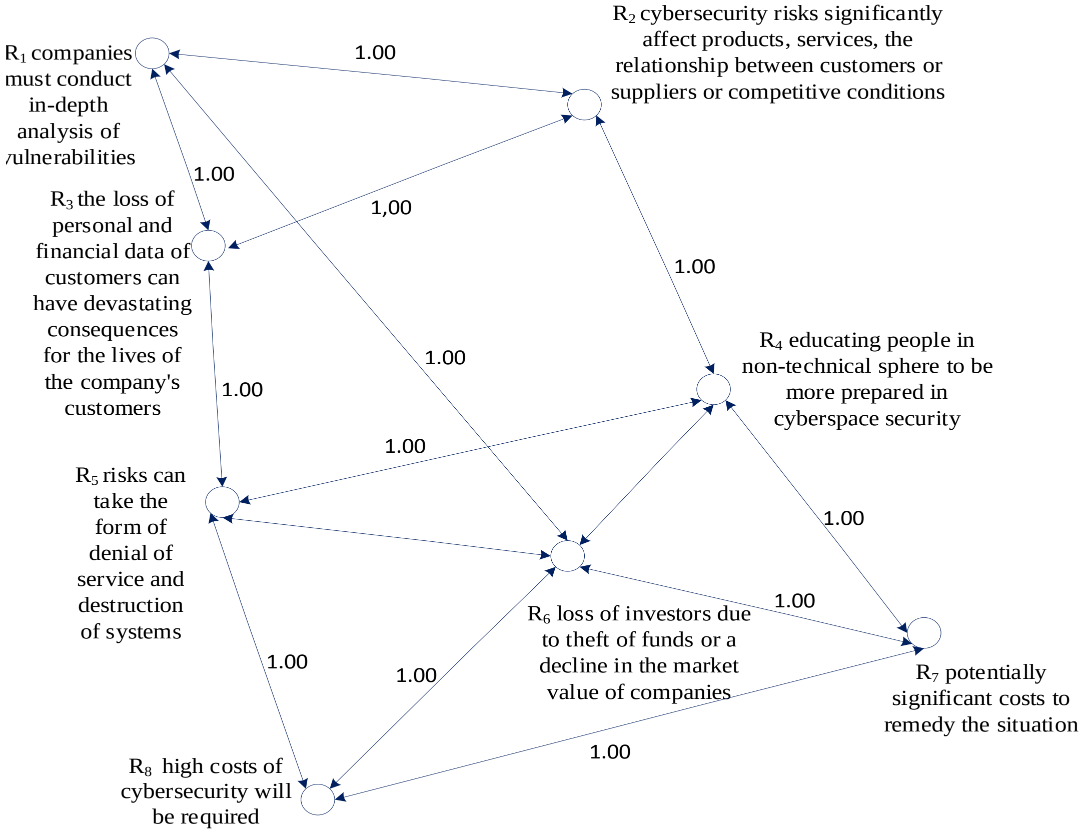

R₁ companies must conduct in-depth analysis of vulnerabilities
R₂ cybersecurity risks significantly affect products, services, the relationship between customers or suppliers or competitive conditions
R₃ the loss of personal and financial data of customers can have devastating consequences for the lives of the company's customers
R₄ educating people in non-technical sphere to be more prepared in cyberspace security
R₅ risks can take the form of denial of service and destruction of systems
R₆ loss of investors due to theft of funds or a decline in the market value of companies
R₇ potentially significant costs to remedy the situation
R₈ high costs of cybersecurity will be required
1.00
1.00
1,00
1.00
1.00
1.00
1.00
1.00
1.00
1.00
1.00
1.00
1.00

Fig 4. – The interaction of the blocks in Model 3 "Cyber risks".

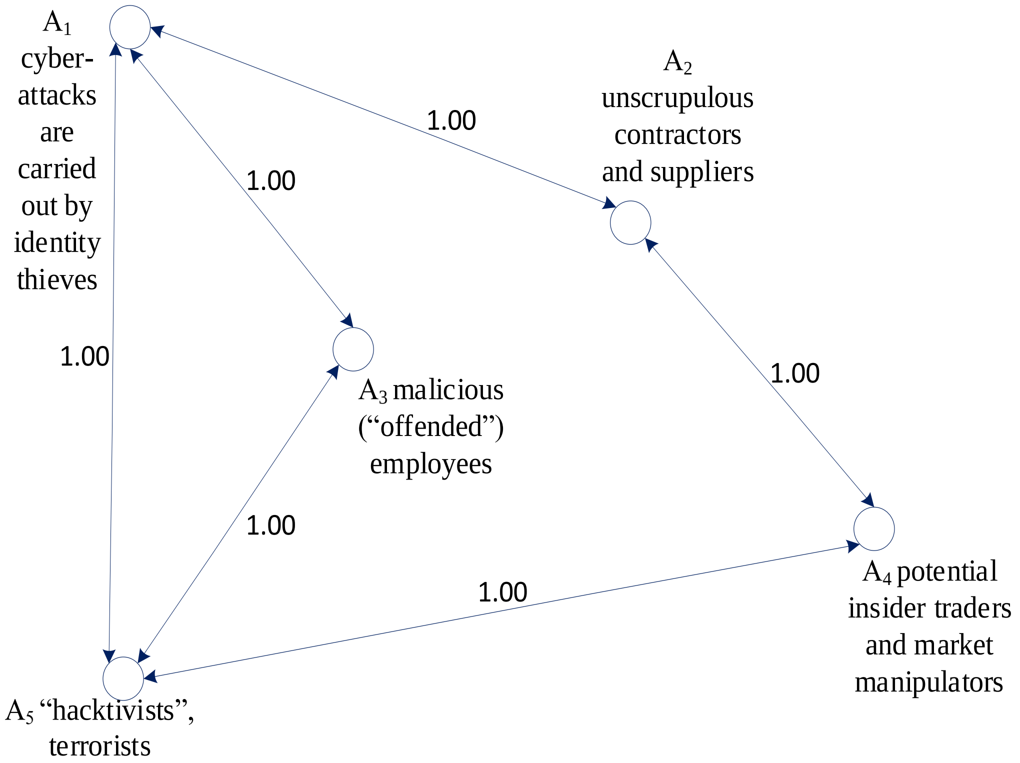

A_1 cyber-attacks are carried out by identity thieves
A_2 unscrupulous contractors and suppliers
A_3 malicious (“offended”) employees
A_4 potential insider traders and market manipulators
A_5 “hacktivists”, terrorists
1.00
1.00
1.00
1.00
1.00
1.00

Fig 5. – The interaction of the blocks in Model 4 "Cyber attacks".

Discussion.

In fig. 1-5 cognitive maps are presented that clearly demonstrate the relationship of the blocks obtained in the course of the analysis of social practices associated with the conduct of potential reflexively controlled cyberwarfare.

In the course of cognitive modeling, we built a cognitive map "Modern cybersecurity" and identified additional links between blocks that have mutual influence on each other: $K_2 + P_4$, $K_3 + A_1$, $K_4 + A_5$, $K_7 + P_3$, $K_7 + R_5$, $R_4 + A_4$, $R_8 + P_1$, $K_7 + P_3$, $K_6 + P_3$, $A_2 + P_4$, $A_1 + P_3$, $K_7 + A_1$ (fig. 6).

Thus, an increased emphasis on cybersecurity for all companies focused on receiving, processing and storing data will lead to the fact that higher costs of cybersecurity will be required, which in turn will harm the company's profit from the position of its lowering and may prevent the free cash flow in the foreseeable future.

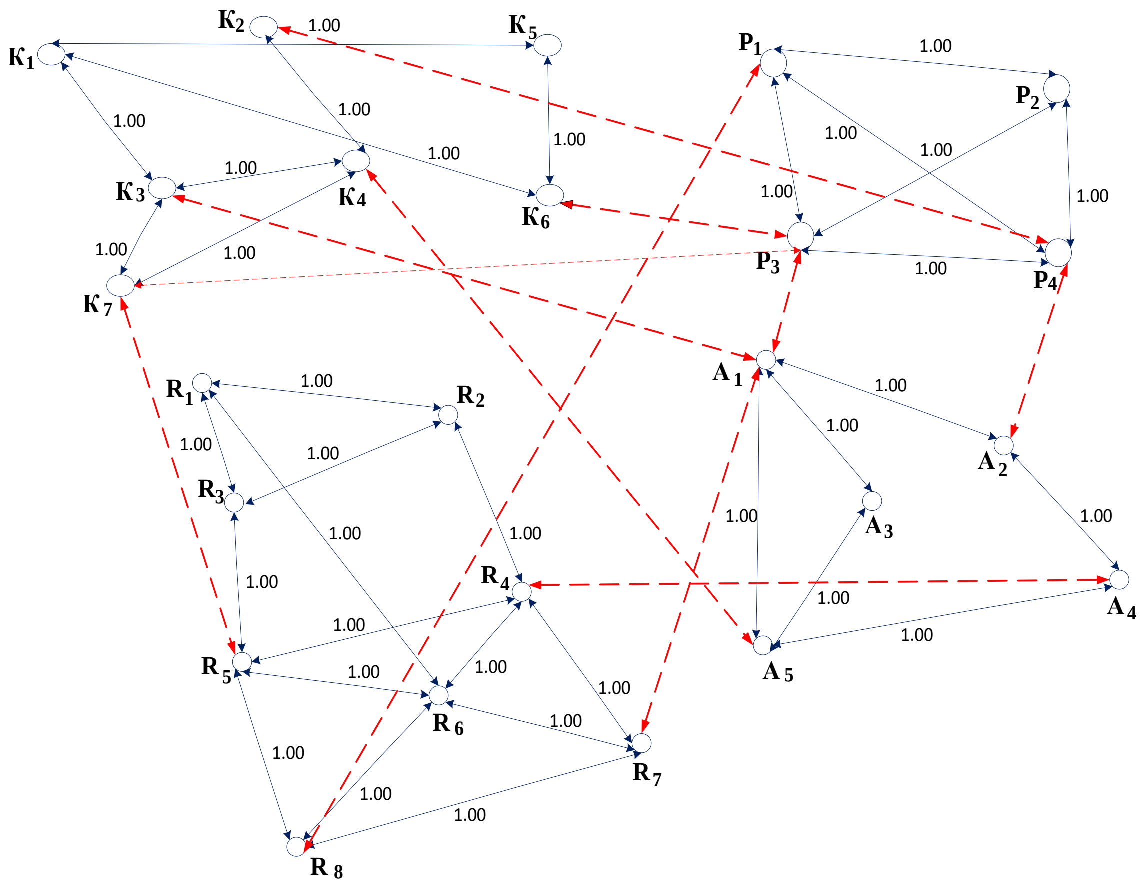


Fig 6. – Cognitive Map of "The modern cybersecurity" model.

Conclusion.

It is worth noting here that cyberattacks are currently focused not only on stealing data, but also on modifying it without detection. Moreover, successful interaction with adversaries in cyberspace requires constant striving for tactical, operational and strategic initiative. It should also be noted that the definition of a national cybersecurity protocol should be the top priority in matters related to ensuring the national security of the state.

References

1. Barabanov, M., Konovalov, I., Kudelev V., Tseluyko, V. Chuzhiye voyny [Alien wars], edited by. R. Pukhova. URL: litvek.com/book-read/253226-kniga-mihail-sergeevich-barabanov-chuzhie-voynyi-chitat-online?p=1

2. Titarenko, I. N. Strakh pered religioznym terrorizmom v Rossii kak fenomen obshchestvennogo soznaniya. [Fear of religious terrorism in Russia as a phenomenon of public consciousness]. Trudy VIII mezhdunarodnoy nauchnoy konferentsii «Innovatsii v nauke i obrazovanii – 2010», posvyashchennoy 80-letiyu obrazovaniya universiteta. Kaliningrad, 19 – 21 oktyabrya 2010. S. 194. s. 194-197.

3. Kemal′ A., Kibervoyna. Kak Rossiya manipuliruyet mirom [How Russia manipulates the world]. 2015. URL: bookash.pro/ru/book/47536/kibervoina-kak-rossiya-manipuliruet-mirom-andrei-kemal

4. Savin, L. V. Strely kentavra. Kibervoyna po-amerikanski. Izdatel′skiy dom «Kislorod» [Centaur arrows. Cyberwar in the American way], 2020. URL: litmir.me/br/?b=688013&p=1

5. Pernik P. Preparing for Cyber Conflict: Case Studies of Cyber Command. Tallinn: International Centre for Defence and Security, December, 2018. URL: icds.ee/wpcontent/uploads/2018/12/ICDS_Report_Preparing_for _Cyber_Conflict _Piret_Pernik_December_2018-1.pdf

6. Brooks, R., How Everything Became War and the Military Became Everything: Tales from the Pentagon. Simon Schuster, 2016. 448 p.

7. Thomas, R., Foreign Policy, March/April 2012. URL: foreignpolicy.com/articles/2012/02/27/cyberwar#6

8. Joseph, N. S. Jr. The Future of Power. New York: Public Affairs, 2011. p. 300.

9. British intelligence mining data from nine U.S. Internet companies in broad secret program. June 7, 2013. URL: washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

10. Microsoft. Report on law enforcement requests. Queries by country/region. URL: microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

11. Diogenes, Yu., Ozkaya E., Cybersecurity: Attack and defense strategies [Cybersecurity: Attack and defense strategies], edited by D. A. Belikova. M.: DMK Press, 2020. p. 326.

12. Gellman B., Soltani A., Washington Post, October 30, 2013, URL: washingtonpost.com/world/national-security/nsa-infiltrates-linksto-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/

13. Khaking, E. D. Iskusstvo eksployta [The Art of the Exploit]. 2-e izd. SPb.: Piter, 2018. p. 496.

14. Jonathan, K. Training staff to be wary of a cyber threat is not a clear-cut job. June 28, 2021. URL: cnbc.com/2021/06/28/training-staff-to-be-wary-of-a-cyber-threat-is-not-a-clear-cut-job.html?&qsearchterm=cyber

15. Weinbaum, C., Shanahan, N.T. John. Intelligence in a Data-Driven Age Joint Force Quarterly, Vol. 90, 3rd Quarter (2018). P. 5.

16. Huntington, S. P., National Policyand the Transoceanic Navy, U.S. Naval Institute Proceedings, 1954. 80, no. 5

17. Maksimov, V.I., Strukturno-tselevoy analiz razvitiya sotsial′no-ekonomicheskikh situatsiy [Structural and target analysis of the development of socio-economic situations]: avtoreferat dis. ... doktora tekhnicheskikh nauk: 05.13.10 / In-t problem upr. im. V.A. Trapeznikova RAN. Moskva. 2002. 54 p.

18. Ginis, L. A. Inzhenernyj vestnik Dona. 2013. № 3. URL: ivdon.ru/uploads/article/pdf/IVD_69_ginis.pdf_1806.pdf

19. Lapshina, I.V., Pershonkova, E.A. Inzhenernyj vestnik Dona. 2021. № 9. URL: ivdon.ru/ru/magazine/archive/n9y2021/7187.