УДК 004.05(075.8)
Луцький національний технічний університет[1)]
Університет Бєльсько-Бяли, Польща[2)]
Андрущак І.Є., Кошелюк В.А., Ящук А.А., Потейчук М.І. [1)], Марценюк В.П. [2)]

INFORMATION SECURITY: KEY THREATS AND REMEDIES.

Андрущак І.Є., Кошелюк В.А., Ящук А.А., Потейчук М.І., Марценюк В.П. Інформаційна безпека: ключові загрози та засоби запобігання. В статті приведено обгрунтування проведення інформаційного аналізу тенденцій розвитку кібератак. Виділені фактори, що, найімовірніше, найбільше позначаються на коливаннях інтенсивності атак. Проведені аналіз факторів впливу на кількість кібератак на інформаційну безпеку web-ресурсів за останні кілька років. Зроблені висновки щодо отриманих результатів і обгрунтовані шляхи підвищення достовірності результатів у подальших дослідженнях.
Ключові слова: кібератака, web-техології, технології захисту, інформаційна безпека.

Андрущак И.Е., Кошелюк В.А., Ящук А.А., Потейчук М.И., Марценюк В.П. Информационная безопасность: ключевые угрозы и средства защиты. В статье приведены обоснования проведения информационного анализа тенденций развития кибератак. Выделенные факторы, которые скорее всего, больше сказываются на колебаниях интенсивности атак. Проведенные анализ факторов влияния на количество кибератак на информационную безопасность web-ресурсов за последние несколько лет. Сделаны выводы о полученных результатов и обоснованны пути повышения достоверности результатов в дальнейших исследованиях.
Ключевые слова: кибератака, web-техологии, технологии защиты, информационная безопасность.

Andrushchak I.Ye., Koshelyuk V.A., Yashchuk A.A., Poteychuk M.I., Martsenyuk V.P. Information security: key threats and remedies. The article gives the justification for conducting an informational analysis of trends in the development of cyber attacks. Allocated factors that are most likely to be most affected by fluctuations in the intensity of attacks. The analysis of the factors influencing the number of cyber attacks on the information-free web-resources over the past few years has been carried out. The conclusions about the obtained results are made and the ways of increasing the reliability of the results in further research are substantiated.
Keywords: cyber-attack, web-teleology, technology of protection, information security.

Formulation of the problem. Modern society enjoys all the benefits of using information technology, which play a crucial role in virtually every human activity. It is obvious that under these conditions the value of cyber security for modern society is extremely high. To date, cybersecurity has ceased to be an issue that worries only specialists in this area. Incidents in the field of cybersecurity affect the lives of consumers of information and many other services, which are also currently well-known for viral attacks or cyber attacks targeted at various objects of electronic communications infrastructure or technology control.

Of great concern is the grave technical and economic consequences of cyberattacks and the tendency to increase their numbers and diversity, which is reflected in statistical reporting in cyber security surveys of world-known companies. Some of these cyber attacks target web resources, in particular the web resources of state-owned enterprises, since they have a political or economic basis.

The number of elements that make up the cyberspace, the large number of interconnections between them, the ability to use special techniques to control the actions of these elements in the form of botnets, for example, determine the potential for the development of threats that are present in the information space. At the same time, all the growing intensity of cyberattacks comes from the magnitude of world cyberspace. Complex attacks have a complex structure, various mechanisms of their implementation and rely on the possibility of using different directions of dissemination of information. Using methods of social engineering allows you to find the most productive methods of attack organization. In cyberspace, as predicted by the experts, increasingly dangerous and complex threats can develop, which makes the task of their comprehensive analysis and use of the results of its solution effective for counteracting existing and possible future cyber threats [1].

Analysis of research. The trends in the development of cyberattacks change year after year and at first glance are quite random. We can analyze them on reports of reputable companies in this area, such as Positive Technologies and Cisco, which are regularly published every quarter of the year. Reports and reviews on cyberattacks contain rather detailed statistics, but they do not make it possible to find a cause-and-effect relationship between the various factors, parameters and effects of cyber attacks only by looking at them.

In order to investigate the patterns of preparation and conduct of cyber attacks and to identify the relationship between them and the influence of various factors, in our view, a correlation and regression analysis of such data and specific factors characterizing cyber attacks should be conducted. These types of

analysis are an example of the most important and popular quantitative methods of mathematical modeling, whose purpose is to establish the existence or absence of a certain connection between random variables or processes and the identification of a functional connection, that is, the form of this dependence. In order to determine the main trends in the development of cyber attacks, it is necessary to check the correlation between the number of detected attacks and factors, which likely to affect fluctuations in the intensity of attacks [2].

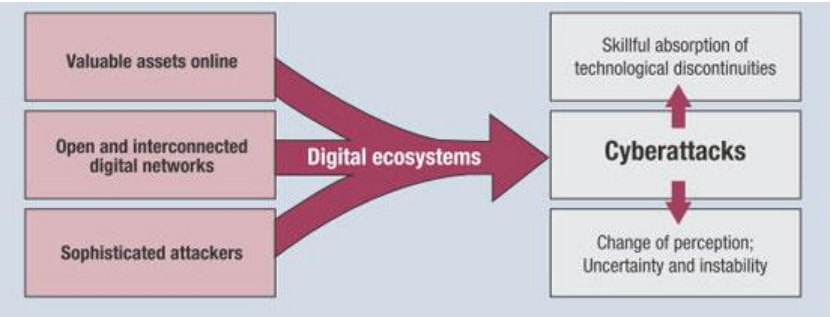
Presentation of the main material and the justification of the results. So what is information security? Usually, it is understood as the security of information and the entire company from deliberate or accidental actions, resulting in damage to its owners or users. Ensuring information security should be aimed primarily at preventing risks, and not at eliminating their consequences. It is the taking of precautionary measures to ensure confidentiality, integrity, and accessibility of information that is the most correct approach in creating an information security system. Any leakage of information can lead to serious problems for the company - from significant financial losses to complete liquidation. Of course, the problem of leaks did not appear today; industrial espionage and the enticement of qualified specialists existed even before the era of computerization. But it was with the advent of the PC and the Internet that new methods of illegally obtaining information appeared. If earlier it was necessary to steal and take out whole bales of paper documents from a company, now huge amounts of important information can be easily merged onto a flash drive placed in a purse, sent over the network, using the family of rootkits, Trojans, backdoors, keyloggers and botnets, or simply destroy through viruses, sabotage.

The development of network technologies is causing an increase in the number of hacker cyber attacks. About 97% of companies were subjected to hacker attacks related to hacking network security tools. Modern firewalls are capable of repelling most intrusions, but some attackers find loopholes due to excellent preparation and carefully planned actions. Tactics of hackers may differ, but in most cases they contain the following steps.

The first step in any cyber attack is intelligence, during which an attacker collects as much information as possible about a company that has become a target for hacking. The information found is necessary to identify vulnerabilities, the hacker performs an analysis of the company's website and its information systems, and also considers ways to interact with other organizations. Once the vulnerability is found, the selection of tools for hacking and preparation for their use begins. For example, one of the ways malware is spread is sending phishing emails.

Once a weak spot has been found in the perimeter of the protection of the target company, which will allow access, the scanning stage begins. For this purpose, publicly available Internet scanning tools are used to detect open ports, software vulnerabilities, equipment configuration errors and other “holes”. This stage can last for months, because the search must be accurate and not provoke the security service to enhance protection. Once a weak spot has been found in the perimeter of the protection of the target company, which will allow access, the scanning stage begins. For this purpose, publicly available Internet scanning tools are used to detect open ports, software vulnerabilities, equipment configuration errors and other “holes”. This stage can last for months, because the search must be accurate and not provoke the security service to enhance protection.

Once a vulnerability has been found and the system has been hacked, it is necessary to guarantee access support for the time required to perform criminal tasks. The company's security service is qualified to detect an attack, so sooner or later the penetration will be revealed. No matter how the hacker tries to hide his presence, it can be issued by operations for moving data within the network or to external resources, disruption of communication between the data processing center and the company's network, establishing connections through non-standard ports, abnormal server or network operations. Network monitoring and traffic analysis (MTA) systems can detect such activity and take measures to prevent it (Pic. 1).



Pic 1. Value realization of a cyberattack

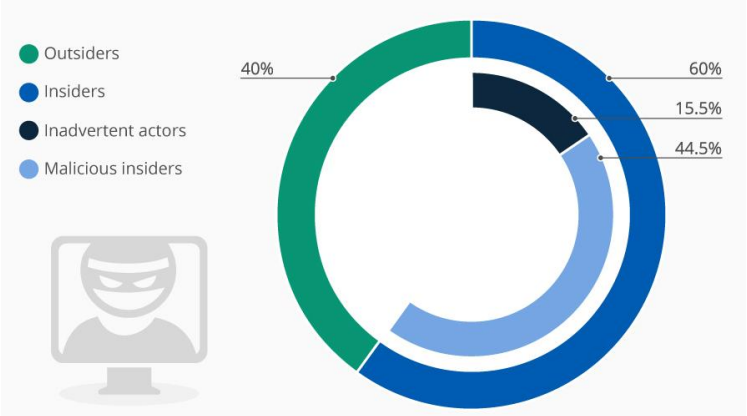
The purpose of an attack in most cases is to gain access to protected resources of the company, such as financial documents or confidential data. Such tools, the rainbow table, allow an attacker to gain administrator access and log on to any information system with elevated privileges, and then gain complete control over the network [3-4].

Not every cyber attack contains this stage. In some cases, the attacker only copies the data for resale, for example. However, at this stage, the hacker already fully controls the network and information systems of the company, and therefore is capable of disabling equipment, erasing databases, shutting down working services and thereby causing enormous material damage and damage to reputation. After an attack is made, it seems reasonable to delete all information about your presence, but in practice this is not always the case. Often, hackers leave signs of hacking as an autograph on their crime, but there is a more practical goal - to confuse the tracks. There are many ways to put experts who are investigating a crime on the wrong path: cleaning and replacing journal entries, creating zombie accounts, using Trojan commands, and others.

At the present stage, a cyber attack should be qualified not only as a crime against information resources, but also as a modern form of committing an act of aggression. By carrying out this type of attack, information constituting state secrets can be stolen, the state's life-support system is disrupted, and such a serious sabotage as the destruction of the anti-missile defense system can be committed, which is a threat to the security of the state and is a violation of generally accepted principles international law. Identifying the perpetrators of such attacks is problematic. However, it is necessary to further develop the existing regulatory framework in this area for the development of international acts, enshrining the rules of responsibility for this crime. Knowledge of the strategy of intruders will detect it at any stage and prevent it in time. Telecom operators should not only rely on their experience in building secure networks, but also use special equipment to monitor and prevent intrusions [5].

One of the most popular cyber attacks is "denial of service" (DDoS), which recently not only causes damage to the attacked company, but also becomes financially motivated. According to a Corero study, 62% of respondents related to network security admit the possibility of transferring money to hackers to stop a DDoS attack on company resources. If earlier such attacks were carried out in order to damage the reputation of the company or to steal data, then now they have become a business, like extortionists for personal computers. Corero also found that almost three-quarters of respondents (73%) expect increased security measures from Internet service providers and believe that they do not protect their customers from DDoS threats.

At the present stage, for the commission of such a serious international crime as aggression, there are various types of weapons, starting with firearms and ending with nuclear weapons. However, it is also necessary to consider this type of attack, as a result of which the life support system of an entire state can be violated and even the work of the antimissile defense system is undermined, which is a violation of state sovereignty and an act of aggression. This type of attack is a cyber attack. As French author D. Ventre points out in his scientific work, "a cyber attack is a modern form of aggression perpetrated by individuals or a whole group of individuals whose goal is to undermine the security information system, undermine the work of any infrastructure, computer network and / or undermine the work personal computers and other devices produced by any means. Cyber attacks are carried out anonymously by attackers, which does not exempt the perpetrators from responsibility; Cyber attacks are illegal entry into someone else's computer system, which can cause a national security system to be undermined. Accordingly, it is problematic to determine the circle of persons guilty of this crime (Pic 2).

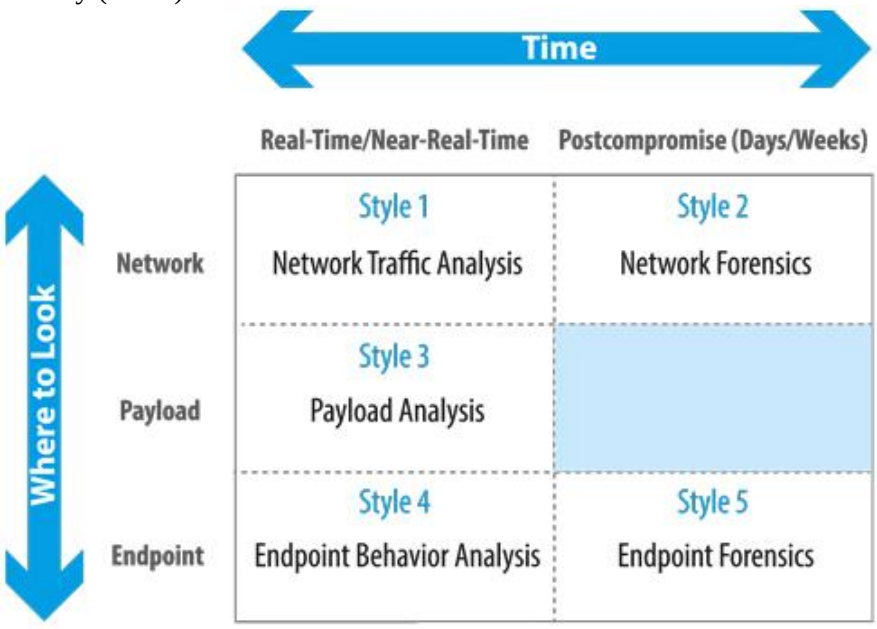


Pic 2. Most Cyber attacks are an inside job

Cyber attacks come in many forms, but they are all a great threat. One of the common types is cyber espionage. In his scientific work, Professor Brenner notes that under cyber espionage, one should qualify activities aimed at obtaining secret service information from the personal data of individuals, groups, or hacking into the system of government service for military purposes, economic or political, using illegal methods of operating the Internet, computer networks or software. As a result of such a cyber attack, secret information, unreliably processed, can be intercepted and even changed, which makes cyber espionage from anywhere in the world feasible. This secret information, falling into the hands of a potential aggressor, can be used in illegal activities against other states, undermining their state and social system, which is a direct manifestation of aggression and a violation of international principles of law. It should also be noted that in recent times, the security services of Ukraine have identified an attempt to commit cyber espionage in order to "infect" the information resources of state authorities and authorities, scientific and military institutions, defense industry enterprises and other objects of critical parts of the country's infrastructure [6].

Another type of cyber attack, which poses even greater threat to the state, is sabotage - undermining the operation of a computer system or satellite systems that perform tasks to maintain the national security of states. In the case of cyber-booting, satellite and computer security systems and life support of the whole state can be endangered: power plants, water supply system, fuel system, transport infrastructure - everything can be at risk. Professor Brenner points out that the civilian sector is also under threat, since criminal activities to undermine security systems have already gone beyond the simple theft of credit card numbers, and a potential target could also be electrical networks, trains, or the stock market. Besides the civilian sphere, the work of the Armed Forces support system can be undermined in order to entail the "disarming" of the whole state [7].

International legal activity aimed at combating cyber-attacks has many obstacles due to the insufficiently developed legislative framework in this area. It should be noted that there is no universally accepted international act on cyber security, and many international lawyers believe that it is urgent to adopt an international treaty in the field of combating cyber attacks. They believe that the international community should consider the issue of cybersecurity as one of the main ones, since this is a global threat for the entire international community (Pic. 3).



Pic 3. Realization of a cyberattack

For example, in his article I.M. Rassolov notes that "among the many problems of judicial practice in these cases, two key issues can be distinguished:

1) the difficulty of determining the circle of persons brought to legal responsibility;

2) fixation (collection, presentation of evidence, their admissibility and reliability.

The main problem in the development of a unified act on the prohibition of cyber attacks is the fact that regardless of the type of attack, it is almost impossible to find out exactly who is the organizer of this attack: single hackers, organized hacker groups or government structures. In view of the high degree of threat to the security of states, which is a cyber attack comparable in level to the consequences of an armed attack, the Tallinn Guide of the second version deals with the norms of international law applicable to such

cyber operations, as well as the conditions under which the general principles of international law will apply as sovereignty, jurisdiction and prohibition of interference in the internal affairs of a state in the context of cybersecurity [8-9].

The number and sophistication of information security threats is growing every year. Despite the fact that the information security services industry is developing, attackers sometimes still manage to be one step ahead. And this happens not because there are no effective remedies or qualified consultants capable of solving the problem. Rather, it comes from the fact that company leaders do not fully understand the need to protect information resources. It is not enough just to install antivirus programs and restrict access to certain data. To ensure maximum confidentiality of information, it is necessary to create a multi-level system for its protection, and not always the company's own IT department can cope with this task. In this case, specialized companies that professionally deal with the protection of information resources come to the rescue.

It is believed that in the modern world it is extremely difficult to protect oneself from cyber attacks. At the same time, cyberattacks always point to vulnerabilities in the system. Due to the research conducted, we were convinced that the weaknesses of the organization of automated accounting at domestic enterprises, in this context, are both normative and software, as well as the entities that they develop and provide support they use (accountants , financiers, etc.). The problem is also the inability of process participants to unauthorized interruptions in their computer networks, lack of knowledge on how to respond adequately to avoid this force majeure and reduce costs of an enterprise in the event that an attack has occurred or is such a threat in the future . Therefore, further efforts need to be focused on a detailed study of the structure of such expenditures in order to minimize their magnitude, as well as the effectiveness of the implementation of preventive costs, in order to avoid those that cause cyberattacks. Thus, it should be concluded that a cyber attack poses a clear threat not only for individual computer networks of any corporations or individuals, but also for computer security systems of an entire state and must be qualified as a modern form of committing an act of aggression, since the consequences of such attacks can be comparable to an armed attack [10].

At the moment there is no single international treaty prohibiting a cyber attack. However, there is a constant work of specialists, legal scholars, whose scientific activities are related to cybercrime, developing recommendatory acts aimed at developing the norms of international law in the field of preventing cyber attacks and establishing responsibility for this crime. It should also be noted the important role of Ukraine, whose international activities are aimed at preserving international peace and security, including in cyberspace. This may mean that developed countries, in contrast to developing countries, have provided themselves with sufficient protection, or this may indicate a change in the political and social causes of cyberattacks. This, unfortunately, suggests an increase in danger for developing countries. However, these conclusions are not clear, since they depend on the correctness of the input data for the analysis.

In general, the results of the information analysis of the factors characterizing the development of cyber attacks can be clarified by expanding and ensuring the adequacy of incoming statistical data. They can also be used to predict the development of cyber attacks and to develop methods and means to counter them.

1. Alders, R. IT Outsourcing: A Practical Guide / R. Alders; trans. with English. - M.: Alpina Business Books, 2003. - 300 p.
2. Agapov V., Yakovlev S., Pratusevich V. Review and assessment of the prospects for the development of the world and Russian information technology markets [Electronic resource] // URL: http://www.moex.com/n8686/?nt=106.
3. Buryachok, V. L. Information and cyber security: the socio-technical aspect: a textbook / [V. L. Buryachok, V. B. Tolubko, V. O. Khoroshko, S. V. Tolyuta]; Per unit edit V. B. Tolubka. - K .: DUT, 2015. - 288 p.
4. Brenner S. Cyber Threats: The Emerging Fault Lines of the Nation State. oxford University Press, 2009.
5. Janczewski L., Colarik A. Cyber Warfare and Cyber Terrorism. Hershey, N.Y.: Information Science Reference, 2008.
6. The Law of Ukraine "On the Basic Principles for the Cybersecurity of Ukraine" - Information from the Verkhovna Rada (VVR), 2017, No. 45, item 403.
7. Heywood, J. Bryan Outsourcing: In Search of Competitive Advantages / J. Bryan Heywood; trans. with English. - M.: Publishing house "Williams", 2004. - 176 p.
8. Tyutina M.V. Analysis and prospects for the development of the information technology market [Text] // Innovative economics: materials IV Intern. sci. Conf. (Kazan, October 2017). - Kazan: Beech, 2017. - P. 9-13.
9. Rid Th. Cyber War Will Not Take Place // Journal of Strategic Studies. 2011.
10. Owens L.L. Justice and Warfare in Cyberspace // Boston Review. A Political and Literature Forum. [Electronic resource] URL: http://bostonreview.net/us/ lisa-lucile-owens-cyber-warfare-national-security.