МРНТИ 20.15.05 https://doi.org/10.58805/kazutb.v.1.22-262

METHODOLOGY FOR REDUCING THE RISKS OF CYBERSECURITY BREACHES AND PROTECTING INFORMATION FROM CYBER ATTACKS

R.I. Vakilov

Armed Forces of the Republic of Azerbaijan, Baku, Azerbaijan,

e-mail: rasimvekilov757@gmail.com

The scientific article examines the problems associated with the risks of cybersecurity violations and information protection from cyber attacks. Given the dramatically increased amounts of information transmitted over networks, the number of cyber attacks is simultaneously increasing, with the aim of stealing various kinds of secret and confidential information. At the same time, the role of specialists involved in the development and implementation of information system security technologies has increased.

The article analyzes vulnerabilities in corporate systems and suggests methods for improving encryption protocols for users' personal data. Special attention is paid to the technologies for implementing protection mechanisms at the software development stage.

Keywords: digital technologies, hacker attacks, cybersecurity, network architecture, protection mechanisms.

КИБЕРҚАУІПСІЗДІКТІҢ БҰЗЫЛУ ҚАУПІН АЗАЙТУ ЖӘНЕ АҚПАРАТТЫ КИБЕРШАБУЫЛДАН ҚОРҒАУ ӘДІСТЕМЕСІ

Р.И. Векилов

Әзірбайжан Республикасы Қарулы Күштері Әскери, Баку, Әзірбайжан,

e-mail: rasimvekilov757@gmail.com

Ғылыми мақалада Киберқауіпсіздіктің бұзылу қаупіне және ақпаратты кибершабуылдан қорғауға қатысты мәселелер қарастырылады. Желілер арқылы берілетін ақпараттың күрт өскен көлемін ескере отырып, әртүрлі құпия және құпия ақпаратты ұрлау мақсатында кибершабуылдар саны бір уақытта артып келеді. Сонымен бірге, ақпараттық жүйелерді қорғау технологияларын әзірлеумен және енгізумен айналысатын мамандардың рөлі артты.

Мақалада корпоративтік жүйелердегі осалдықтар талданады және пайдаланушылардың жеке деректерін шифрлау хаттамаларын жетілдіру әдістері ұсынылады. Бағдарламалық қамтамасыз етуді әзірлеу кезеңінде қорғау тетіктерін енгізу технологияларына ерекше назар аударылды.

Түйін сөздер: Сандық технологиялар, хакерлік шабуылдар, киберқауіпсіздік, желі архитектурасы, қорғаныс механизмдері.

МЕТОДОЛОГИЯ СНИЖЕНИЯ РИСКОВ НАРУШЕНИЙ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОТ КИБЕРАТАК

Векилов Р.И.

ВС Республики Азербайджан, Баку, Азербайджан,

e-mail: rasimvekilov757@gmail.com

В научной статье исследуются проблемы, связанные с рисками нарушений кибербезопасности и защиты информации от кибератак. Учитывая резко взросшие объемы информации, передаваемой по сетям, одновременно увеличивается количество кибератак, с целью хищения различного рода секретной и конфиденциальной информации. Одновременно возросла роль специалистов, занимающихся разработкой и внедрением технологий защиты информационных систем.

В статье анализируются уязвимости в корпоративных системах и предлагаются методы совершенствования протоколов шифрования персональных данных пользователей. Особое внимание уделено технологиям внедрения механизмов защиты на этапе разработки программного обеспечения.

Ключевые слова: цифровые технологии, хакерские атаки, кибербезопасность, архитектура сети, механизмы защиты.

Introduction. The development of digital technologies has led to the emergence of a large number of digital threats on the Internet. For example, the theft of users' personal data or hacker attacks on the company's information systems in order to disable them. In response to threats, a field of knowledge has emerged that is engaged in the development and implementation of technologies to protect information systems from them - cybersecurity. Cybersecurity experts study crimes and threats in the digital environment and develop ways to counter them. For example, they are looking for vulnerabilities in corporate systems and improving encryption protocols for users' personal data.

Materials and methods. According to the forecasts of the service Statista.com The global cybersecurity market will continue to grow and will exceed $650 billion by 2030 Cybersecurity Goals The main goals of cybersecurity are to ensure the security of networks, devices and software. The objects of protection against cyber threats in global networks include, for example, software and databases of companies, network architecture, websites and applications, smartphones, computers, IoT devices like smartwatches and software for managing them(fig.1).

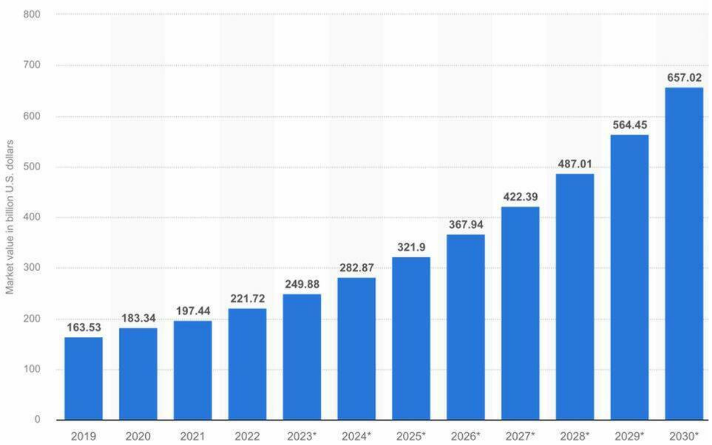

Figure 1 - Projected statistics of an increase in cyber threats

According to the forecasts of the service Statista.com The global cybersecurity market will continue to grow and will exceed $650 billion by 2030 Cybersecurity Goals The main goals of cybersecurity are to ensure the security of networks, devices and software. The objects of protection against cyber threats in global networks include, for example, software and databases of companies, network architecture, websites and applications, smartphones, computers, IoT devices like smartwatches and software for managing them [1].

By hacking them, attackers can disable the systems or steal the data that is stored in them. For example, user contacts, bank card numbers, and even health information. The data can be sold or used for theft or blackmail. For companies, cyberattacks are financial and reputational losses. Criminals can erase customer databases or disclose their personal data on the Internet.

They can steal developments and sell them to competitors, or disable the network architecture and stop the company's work for several days. Cybersecurity specialists implement protection mechanisms at the software development stage and constantly analyze potential vulnerabilities of programs, networks and devices. Protect information Data stored and transmitted on the Internet must be protected from unauthorized access. For example, the username and password, phone number and address that the user enters when registering on the site should not become available to cybercriminals [2]. Any changes to the data must be authorized by their owner. For example, only the user can change the information in the user's account. And only its administrator can add or remove information from the company's customer base. Figure 2 shows the percentage of harmful factors.

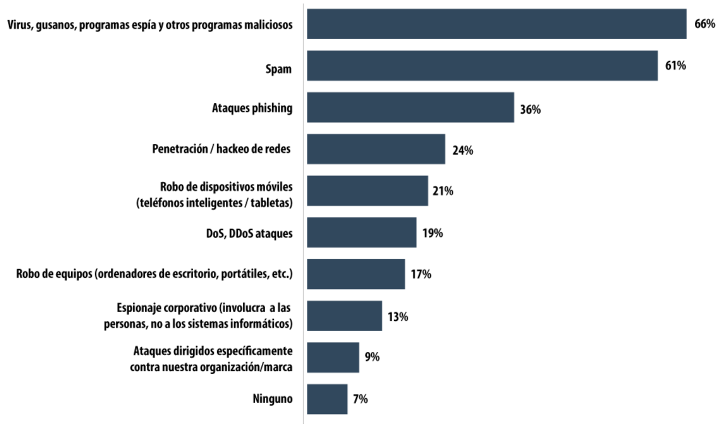

Figure 2 - Percentage of harmful factors

Despite cyber attacks, the data should remain accessible: the user should not lose access to the account, and the company's support service should not lose access to customer contacts from the database.

Detect threats and respond to incidents Incidents are the actions of cybercriminals that can lead to a violation of information security or the failure of information systems. For example, unauthorized access to databases can reveal confidential information [3]. And a large number of requests to the site exceeding the network bandwidth will block its operation. Incident response includes, for example, resetting passwords of a suspicious account and restoring a backup copy of the information system after unauthorized data deletion.

Systems can be subject to cyber threats not only because of internal vulnerabilities, but also because of human errors. For example, if an employee of a company connects to corporate software via a public Wi-Fi network, his username and password can be intercepted by intruders. Or if he logs into his personal email from his work computer and clicks on a suspicious link in the email, he will expose the system to the threat of a virus attack. Figure 3 shows мethods for identifying information flows.

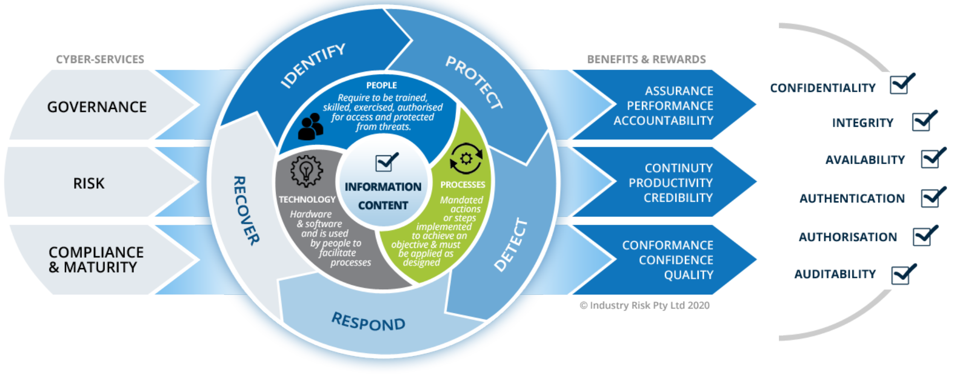
CYBER-SERVICES
GOVERNANCE
RISK
COMPLIANCE & MATURITY
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
PEOPLE
Require to be trained, skilled, exercised, authorised for access and protected from threats.
TECHNOLOGY
Hardware & software and is used by people to facilitate processes
INFORMATION CONTENT
PROCESSES
Mandated actions or steps implemented to achieve an objective & must be applied as designed
BENEFITS & REWARDS
ASSURANCE PERFORMANCE ACCOUNTABILITY
CONTINUITY PRODUCTIVITY CREDIBILITY
CONFORMANCE CONFIDENCE QUALITY
CONFIDENTIALITY ✓
INTEGRITY ✓
AVAILABILITY ✓
AUTHENTICATION ✓
AUTHORISATION ✓
AUDITABILITY ✓
© Industry Risk Pty Ltd 2020

Figure 3 - Methods for identifying information flows

To reduce the risks of cybersecurity violations by employees, you need to teach them the basics of cybersecurity: talk about possible threats, consequences and ways to avoid them.

How does cybersecurity differ from information security?

Information security protects data that can be stored both digitally and on paper. Information security specialists are fighting against external and internal threats. For example, they prevent the consequences of accidental data changes or system malfunctions due to technical failures [4].

Cybersecurity refers to the protection of digital information only and mainly from threats from outside - from Internet networks.

Results and discussions. Information security is a superset of cybersecurity

In the modern world, digitalization has affected all industries and social spheres, so it is impossible to ensure the security of information without protecting it from cyber threats. Information security and cybersecurity are interrelated and complement each other, so in practice the concepts are sometimes used synonymously. Often in companies, especially in small ones, both directions are led by one employee [5].

Criteria for assessing the noise immunity of information systems

Noise immunity is understood as the ability of an information system to withstand the harmful effects of interference. As a result of interference, the received message will differ to some extent from the transmitted one. Therefore, noise immunity can be characterized as the degree of compliance of the received message with the transmitted one at a given interference. When comparing several systems, one of them will be more noise-resistant, which, with the same interference, will provide less difference between received and transmitted messages.

The effect of noise is that some symbols in the signal are replaced by others, as a result of which another signal is received instead of the transmitted signal. The noise immunity of the communication system can be most fully characterized by a set of probabilities {Pik} that when transmitting the i-th signal, the k-th (i, k = 1,2,...,N) will be received; and if we want to set the requirements for the noise immunity of the system, taking into account the value of each of the messages individually, then setting the entire the {Pik} matrix is necessary [6].

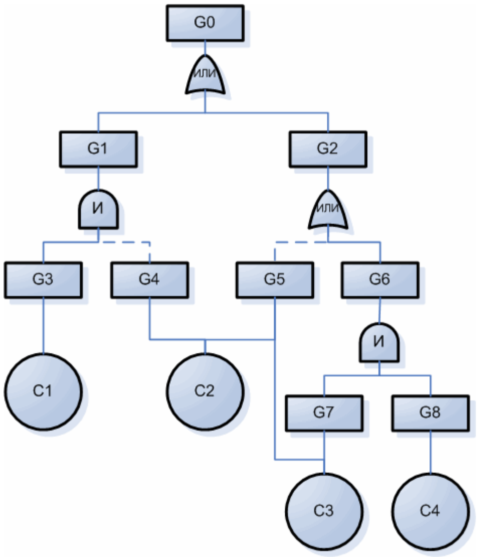

Figure 4 - Attack trees

However, comparing systems by their {Pik} matrices (which can be called ”stochastic message transformation matrices”) is associated with a number of difficulties, and often not necessary: it is enough to introduce simpler noise immunity characteristics. Such simple parameters include, for example, the average probability of an erroneous admission, $P_{\text{average error}}$.

Modeling of information flows

The process of assessing information security using information flow modeling will reveal:

- trends in the behavior of the system;
- the occurrence of potential errors;
- the scale of vulnerabilities;
- The extent of the consequences of the probable threat.

A preliminary assessment of the entire system and identification of potential risks makes it possible to effectively make decisions about security measures.

Attack trees or error trees are a structured and hierarchical way to collect possible threats. The tree describes a possible attack and its purpose, linking the attackers' tasks with the purpose of the attack, as well as possible implementation methods. Attack trees can be used either in conjunction with other analysis tools, or as an independent research tool [7].

The peculiarity of attack trees is that the expert builds a separate attack tree for each software product of the company. Thus, it turns out a whole chain of threats that hackers can “climb” to achieve their goal (Fig. 4).

After analyzing and evaluating the company's information security, specialists will be able to anticipate the likelihood of a threat and the scale of possible damage. As a rule, experts refer to the following data:

- conducted research;
- results of the IB analysis;
- data on previously conducted attacks.

Specialists define two main vectors of work:

1. Eliminate the consequences of the attack, if it is successful.

2. Acceptance and elaboration of risks.

Conclusions. Based on the results of the conducted research, we can determine the level of production costs for eliminating the consequences of cyber threats. Statistics are collected for several reporting periods. They reflect real incidents of data leaks, reputational risks, and the effectiveness of security systems. With the help of the information collected, we decide on the actions that need to be taken to ensure an appropriate level of protection.

When calculating risks, we also pay attention to the cost of eliminating them. If the elimination of the risk exceeds the expected losses, we suggest minimizing possible losses, rather than completely eliminating such a risk. Such an analysis helps to correctly allocate budgets to protect your data and avoid unplanned expenses

Information security analysis and assessment contribute to raising awareness of the degree of protection. Work on studying potential risks and vulnerabilities, as well as actions to minimize them, can improve the security of an organization's data, its networks and servers.

References

1. Algoritm vyjavlenija ugroz informacionnoj bezopasnosti v raspredelennyh mul'tiservisnyh setjah organov gosudarstvennogo upravlenija / A. Ju. Puchkov, A. M. Sokolov, S. S. Shirokov, N. N. Prokimnov // Prikladnaja informatika. - 2023. - T. 18, № 2. - str. 85-102.

2. Vasil'ev V. I. Ocenka aktual'nyh ugroz bezopasnosti informacii s pomoshh'ju tehnologii transformerov / V. I. Vasil'ev, A. M. Vul'fin, N. V. Kuchkarova // Voprosy kiberbezopasnosti. - 2022. - № 2. - str. 27-38.

3. Gladkov A. N. Vizualizacija kiberugroz kak aspekt formirovanija kompetencij v oblasti informacionnoj bezopasnosti = Visualization of Cyber Threats as an Aspect of the Formation of Competencies in the field of Information Security / A. N. Gladkov, S. N. Gorjachev, N. S. Kobjakov // Zashhita informacii. Insajd. - 2023. - № 1. - str. 32-37.

4. Informacionnaja bezopasnost' sovremennogo predprijatija = Information Security of Advanced Company: Password Protection: parol'naja zashhita / M. Ju. Ivanov, M. V. Sygotina, M. Ju. Vahrusheva, V. V. Nadrshin // Zashhita informacii. Insajd. - 2022. - № 6. - str. 62-66.

5. Nazarov D. M. Osnovy obespechenija bezopasnosti personal'nyh dannyh v organizacii: ucheb. posobie / D. M. Nazarov, K. M. Samatov; M-vo nauki i vyssh. obrazovanija Ros. Federacii, Ural. gos. jekon. un-t. - Ekaterinburg: Izd-vo Ural. gos. jekon. un-ta, 2019. -118 s.

6. Savin M. V. Metodika vyjavlenija i ocenki nedopustimyh sobytij na osnove modeli zrelosti upravlenija informacionnoj bezopasnost'ju = Methodology for Identifying and Evaluating Unacceptable Events Based on the Maturity Model

of Information Security Management / M. V. Savin, M. A. Kondratenko // Zashhita informacii. Insajd. - 2023. - № 1. - str. 24-31.

7. Shnjukov A. V. Finansovaja i informacionnaja bezopasnost' pol'zovatelej komp'juterov i smartfonov / A. V. Shnjukov, E. A. Shnjukova // Jekonomika i predprinimatel'stvo. - 2022. - № 1. - str. 1440-1444.

Information about the author

Vakilov R.I. - Senior Assistant to the Military Attache of the Armed Forces of the Republic of Azerbaijan, г. Баку, Азербайджан e-mail: rasimvekilov757@gmail.com.

Сведения об авторе

Векилов Р.И. - Старший помощник военного атташе вооруженных сил Республики Азербайджан, г. Баку, Азербайджан, e-mail: rasimvekilov757@gmail.com