Problematics of protection of information resources of the enterprise

Andrey Gazizov [1*], *Andrey* Filiev[1], and *Vitaliy* Popov[1]

[1]Don State Technical University, 344002 Rostov-on-Don, Russia

Abstract. In the modern era of societal advancement, there is a notable reliance on information and communication technologies within engineering centers. This reliance underscores the importance of implementing effective organizational and technical measures to safeguard information resources. Ensuring compliance with necessary security standards and employing certified protective measures is imperative. Protecting the Engineering Center's information involves continuous monitoring and prompt response to any breaches compromising integrity, confidentiality, and availability. Identifying specific vulnerabilities that directly jeopardize these resources is essential. Moreover, safeguarding resources necessitates a comprehensive protection strategy encompassing software, technical, cryptographic, and organizational measures to uphold information security consistently.

1 Introduction

In today's era of societal advancement, the active utilization of information and communication technologies (ICT) is evident across numerous facets of human endeavor, including within engineering centers. ICT encompasses a broad spectrum of tools and systems, including software, hardware, and technical devices. These components operate on the foundation of microprocessor and computer hardware principles. Furthermore, modern ICT systems encompass a wide array of functionalities, including facilitating information broadcasting, enabling seamless information exchange, and supporting operations related to data collection, production, accumulation, storage, processing, and transfer [1]. Moreover, ICT infrastructure extends beyond local boundaries, providing access to information resources within both local and global computer networks. This expansive reach underscores the interconnected nature of modern technology, allowing for efficient collaboration, resource sharing, and information access across diverse geographical locations and organizational boundaries. Thus, the integration of ICT within engineering centers signifies a pivotal aspect of contemporary societal development, enabling enhanced efficiency, connectivity, and innovation across various industries and sectors [1].

In accordance with the Federal Law "On Industrial Policy in the Russian Federation", an engineering center is a legal entity that provides engineering consulting services for the preparation of the process of production and sale of products (works, services), preparation

* Corresponding author: gazandre@yandex.ru

of industrial and infrastructure as well as other facilities construction and operation , pre-design and design services.

The utilization of ICT tools within the operations of engineering centers necessitates the implementation of effective organizational and technical measures to safeguard information resources. This requirement includes ensuring adherence to appropriate security standards and employing certified methods for information protection to guarantee the integrity and security of data.

Information protection in the engineering center implies continuous monitoring and timely response to incidents related to violation of integrity, confidentiality and availability of information resources.

The Engineering Centre shall have and keep up-to-date the "Information Security Policy" aimed at minimizing the number of attacks by internal and external intruders, including prevention of unauthorized access to information resources [2].

The list of information resources of the Engineering Center is presented in Figure 1:

1) Application and system software.
2) Personal data of employees and customers.
3) Company and customer documentation.
4) Commercial offers and data from electronic auctions.

Engineering Center information resources may be susceptible to the following types of vulnerabilities:

- disclosure of restricted information;
- emergency situation;
- failure to control input or output data;
- failure to maintain equipment;

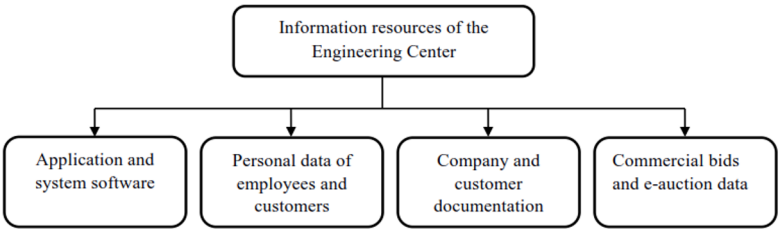

Fig. 1. Information resources of the Engineering Center

- internal and external attackers;
- malfunctioning and disruption of ICT facilities;
- malicious software;
- negligent attitude to the "Information Security Policy";
- personnel errors;
- software failure;
- theft of information transmitted over wired communication lines and wireless network;
- unauthorized access to information;
- violation of information integrity during transmission via local area network [3].

To ensure the smooth operation of the engineering center, prioritizing maximum information security is crucial since even a minor threat can result in significant consequences. Nevertheless, it is not advisable to focus extensively on minor threats, as addressing them may demand excessive resources without yielding substantial benefits for the center.

Once potential threat sources are identified, it becomes essential to conduct an expert evaluation to assess the likelihood of these threats manifesting within the engineering center.

This evaluation involves categorizing the potential consequences of these threats, considering factors such as:

- the frequency of occurrence of each threat.
- the adequacy of protection measures for information resources vulnerable to intrusion.
- the motives behind and methods utilized for actualizing these threats.
- potential threats arising from unforeseen circumstances or force majeure events.

Statistical data of the "threat bank" of the engineering center allows to determine with what frequency the threat occurs and what is targeted.

Conclusion: the engineering center has information resources mandatory for protection; specific vulnerabilities posing a direct threat to them were identified in order to clarify the issues of information resources protection [4].

2 Problematics of information resources protection of the engineering center

2.1 Problems of protection of information resources

Considering the substantial volume of information handled within the engineering center, it is imperative to implement organizational measures aimed at fostering a shared comprehension of the "information protection concept" among center personnel. Additionally, establishing a structured approach encompassing both strategy and tactics for controlling information resource security is essential. This involves conducting training sessions for employees in this domain and furnishing them with detailed guidelines on information security protocols. Moreover, designating responsible individuals to oversee information resource protection and ensure adherence to established protocols by staff members is vital [5].

The purpose of information resources protection is to obtain information on vulnerabilities that may result in destructive actions due to unauthorized access to resources. In practice, information protection occurs under the random influence of various factors. Some of them can be systematized and are described in national standards; while others are initially unknown and can reduce the effectiveness or even negate the envisaged measures to protect information resources. Evaluation of the effectiveness of the implemented information protection mechanisms should include analysis and objective assessment of circumstances, as well as consideration of probabilistic factors [6].

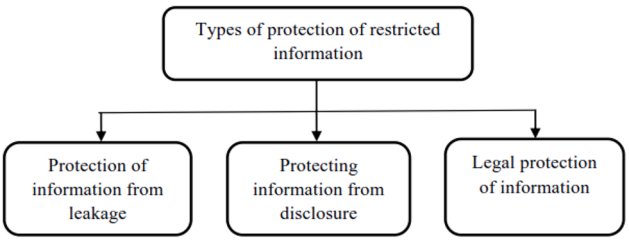

Fig. 2. Types of protection of restricted information

Factors affecting the level of information protection are specified in the State Standard of the Russian Federation "GOST 51275-99". At the same time, when designing information protection systems, there are previously unknown circumstances that can subsequently reduce the effectiveness of information resources protection or compromise the envisioned information security measures.

For this reason, when assessing the effectiveness of information protection, it is necessary to take into account these circumstances and the probabilistic characteristics specified in the State Standard of the Russian Federation "GOST R 50922-96". This methodology is included in the system of normative documents, where there are quantitative and measurable indicators of the effectiveness of information protection means, ensuring the safety of interests of both customers and designers. Control over the effectiveness of the measures taken allows to determine how effectively they are implemented and whether they meet the objectives set for the protection of information resources.

The list of the main types of restricted information protection of restricted is presented in Figure 2:

1) Protection of information from leakage represents a set of measures aimed at preventing uncontrolled dissemination of protected information through unauthorized access to it.

2) Protection of information from disclosure represents a set of measures aimed at preventing unauthorized dissemination of protected information by persons who do not have the right to do so.

3) Legal protection of information is a set of measures aimed at preventing the acquisition of protected information by an interested party in violation of legal norms.

In order to safeguard the information assets of the engineering center, it is imperative to devise a comprehensive "security framework." This framework should encompass software, hardware, cryptographic protocols, and organizational protocols to guarantee the continuous protection of resources against both accidental and intentional threats, while also thwarting any unauthorized access [7].

Information security of the Engineering Centre covers measures aimed at preventing unauthorized access, use, disclosure, distortion, research, change, recording or destruction of information, regardless of its form - electronic or material. The primary focus in guaranteeing the security of information resources revolves around achieving equilibrium among preserving confidentiality, integrity, and accessibility of these resources, all while considering the necessity of protection without hindering the operational efficiency of the Engineering Center. This equilibrium is attained through risk management, involving the identification of information resources and potential threats, evaluation of vulnerabilities and their possible consequences, and the formulation of a strategy for mitigating these risks. Information security of the Engineering Center implies ensuring confidentiality, integrity and availability of information resources at the necessary and sufficient level [8].

The problems of protecting information resources today are associated with various kinds of vulnerabilities, the list of which is replenished regularly. Internal and external intruders have different opportunities to implement unauthorized access to resources and exploit successfully the vulnerabilities that exist in the information system. At the same time, illegal actions can be carried out by an intruder and be aimed at obtaining confidential information; as well as determined by carelessness or inexperience of engineering center employees, causing damage to the reputation of the center, its financial component, as well as personal data of clients and employees. The primary challenge regarding the protection of information resources at the Engineering Center revolves around the necessity for substantial financial resources to attain the requisite level of security.

The list of actual problems of information resources protection of the engineering center is presented in Figure 3:

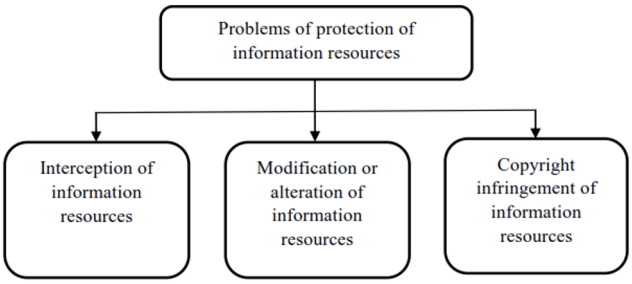

Fig. 3. Problems of protection of information resources

1) Infringement of copyright in information resources. This problem can have serious consequences. For example, an employee or a client of an engineering center can send a letter on behalf of the manager (this type of fraud is called "spoofing"); or a Web-server, which receives a request from an enterprise-client, can turn out to be a "phishing" site, where confidential information is requested - data on orders, bank card numbers and other information, while the "phishing" site itself does not respond to the requests received.

2) Interception of information resources transmitted over a network. In this case, the attacker violates the confidentiality of information, while the integrity of such information remains unchanged.

3) Modification or alteration of information resources. In this case, the attacker changes the original meaning of the transmitted message or completely replaces (substitutes) the resource [9].

Nowadays, methods of cryptographic protection of information resources are used more and more often, but it contradicts the interests of end users and the requirements of the "Security Policy" of the Engineering Center.

The practice of using information resources significant number of possible ways of their leakage in information systems:

- attacks at the local level;
- channel and packet switching errors;
- copying data from external media;
- deliberate disabling of "information security mechanisms";
- exploitation of operating system vulnerabilities;
- hidden requests of intruders in the system;
- impersonation of "legitimate" users by attackers;
- implementation of program traps;
- program bookmarks;
- reading of final information in the permanent storage device of an information system after the fulfillment of requests authorized by the system;
- unauthorized access to ICT facilities and communication lines;
- use of malicious software.

To safeguard the information resources of an engineering center, it is advisable to implement the following organizational security measures:

- restriction of physical access to premises where restricted information is processed;
- destruction of used data carriers;
- installation of coded locks at the entrance to the protected premises.

Physical means of protection of information resources of an engineering center represent complex security systems of information objects, including access control systems and room shielding; application of acoustic information protection methods [11].

Protection of engineering center resources within the perimeter of the information system is implemented by means of various hardware and software:

- allocation of control bits for records in order to identify information;
- blocking of key and information input;
- control of access to the information system memory by differentiating access to information;
- detection of errors during information transfer to the network.

To successfully carry out an attack on the information resources of an engineering center, the attacker employs various tools, including software such as "viruses" and "spyware". These programs record user actions, thereby exploiting vulnerabilities in the information system. Most anti-virus programs cannot detect malicious code, so it is necessary to use information security software that has been tested and has certificates of conformity. In some cases, the realization of intercepting and gaining access to protected information does not allow the attacker to fully perform the "destructive" task that is in front of him. When examining network traffic in an engineering center, an attacker is able to obtain information about the information system, but is unable to manipulate the information because more information about it is required for successful interception [15].

2.2 Objectives of information resources protection

With the development of the global network "Internet", there are new problems with the security of information resources. Modern technologies allow an attacker to carry out an attack from anywhere in the world, leaving the information system unnoticed; for this reason, when investigating an incident, it is difficult or impossible to determine how and where territorially the attack was made.

Tasks to ensure the security of information resources of the engineering center should be focused on the following activities:

- to ensure confidentiality, integrity and structuring of information;
- to develop and keep "up-to-date" the Center's Security Policy;
- to identify and prevent external and internal threats to information in a timely manner;
- to implement organizational, software-hardware and engineering-technical methods to enhance information protection [13].

Ensuring the security of information resources for the Engineering Center is a very urgent task. In order to ensure the required level of resources security and minimize the loss of resources in case of implementation of a successful attack of an intruder, it is necessary to perform the following tasks:

- to continuously monitor the identification of information security threats and take preparatory measures to eliminate them;
- to develop a "Risk Management Plan" in the field of information protection and implement it in the main "business processes" of the center;
- to keep an electronic log of information protection from unauthorized access;
- to modernize the existing means and systems of information protection at the enterprise;
-to promptly respond to abnormal situations related to unauthorized access to information and violation of the "workflow of the center";
-to timely update and reissue normative documents, local acts of the Center related to information protection, regulating information security of the Engineering Center;
- to activate the work of the information protection unit by submitting the necessary additional authorizations;
- to timely carry out activities on training and informing employees in the field of information protection [14].

Thus, it seems possible to identify the most significant tasks, which determine the measures for the analysis of protection methods from unauthorized access to the information

resources of the center and internal and external threats; including the identification of vulnerabilities of the information system of the center:

- identification of actual threats and vulnerabilities of the information system within the perimeter (protected - segment, local area network).
- identification of possible threats of unauthorized entry and movement around the enterprise of unauthorized persons and their access to the resources of the information system;
- identification of threats and vulnerabilities of the information system in the global network "Internet" (official site, wireless and wired network).

The "Security Policy" document [15,17] contains comprehensive details regarding the most susceptible components of the engineering center's information system. This information is essential for conducting further analysis aimed at devising methods to protect these resources.

3 Conclusion

In order to protect the information resources of the Engineering Center and minimize the risks of loss of these resources, it is necessary to introduce a set of information protection measures and practical implementation of protection means; and, based on the identified vulnerabilities of the information system, the regulation of "protection measures" should be observed. It is necessary to justify the objectives of information protection and identify those information flows that contain information with restricted access.

References

1. A. Azizi, H. Laaji, Journal of Cyber Security and Mobility 725–744 (2021) https://doi.org/10.13052/jcsm2245-1439.1045
2. A. Hülsing, J. Rijneveld, J. Schanck, P. Schwabe, CHES 2017; Springer International Publishing: Cham, Switzerlamd, 232–252 (2017) https://doi.org/10.1007/978-3-319-66787-4_12
3. M. Imran, Z.U. Abideen, S. Pagliarini, Electronics **9**, 1953, (2020) https://doi.org/10.3390/electronics 9111953
4. Malina Lukas et al. *On the Efficiency and Security of Quantum-resistant Key Establishment Mechanisms on FPGA Platforms*. International Conference on Security and Cryptography, pp. 605-613 (2022) https://doi.org/10.5220/0011294200003283
5. F. Farahmand, M. U. Sharif, K. Briggs and K. Gaj, *A High-Speed Constant-Time Hardware Implementation of NTRUEncrypt SVES*. International Conference on Field-Programmable Technology (FPT), Naha, Japan, pp. 190-197. (2018) https://doi.org/10.1109/FPT.2018.00036.
6. Y. Zhu, Y. Liu, M. Wu, J. Li, S. Liu, J. Zhao, Electronics **11**, 856 (2022) https://doi.org/10.3390/electronics11060856
7. O. M. Guillen, T. Pöppelmann, J. M. Bermudo Mera, E. F. Bongenaar, G. Sigl, J. Sepulveda, *Towards Post-Quantum Security for IoT Endpoints with NTRU*. Design, Automation & Test in Europe Conference & Exhibition (DATE), Lausanne, Switzerland, 2017, pp. 698-703, (2017) https://doi.org/10.23919/DATE.2017.7927079.
8. E.H. Laaji, A. Azizi, S. Ezzouak, *Two Quantum Attack Algorithms Against NTRU When the Private Key and Plaintext Are Codified in Ternary Polynomials*. Innovation in Information Systems and Technologies to Support Learning Research.

EMENA-ISTL 2019, Springer, Cham, pp. 551-562 (2020) https://doi.org/10.1007/978-3-030-36778-7_61

9. J. Hoffstein, J. Pipher, J.M. Schanck, J.H. Silverman, W. Whyte, Z. Zhang, Lecture Notes in Computer Science Springer, Cham, **10159**, 3-18 (2017) https://doi.org/10.1007/978-3-319-52153-4_1
10. P. Razumov, O. Safaryan, L. Cherckesova, et al. E3S Web of Conferences **224**, 1–9 (2020) https://doi.org/10.1051/e3sconf/202022401037.
11. S. An, S. Kim, S. Jin, H. Kim, H. Kim, Applied Sciences **8(11)**, (2018) https://doi.org/10.3390/app8112014
12. İ. Keskinkurt Paksoy and M. Cenk, *Faster NTRU on ARM Cortex-M4 With TMVP-Based Multiplication*. IEEE Transactions on Circuits and Systems I: Regular Papers, **69(10)**, pp. 4083-4092 (2022) https://doi.org/10.1109/TCSI.2022.3191111
13. H. Cheng, J. Großschädl, P. B. Rønne and P. Y. A. Ryan, *AVRNTRU: Lightweight NTRU-based Post-Quantum Cryptography for 8-bit AVR Microcontrollers*. 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, pp. 1272-1277 (2021) https://doi.org/10.23919/DATE51398.2021.9474033.
14. R. Y. Hassan, N. Z. Hany, H. A. Hadeel, A. M. Ismail, I. E. Wageda, Applied Mathematics & Information Sciences And International Journal **17**, 49-53 (2022) https://doi.org/10.18576/amis/170107
15. S.H. Shahhadi, H.R. Yassein, Journal of Physics: Conference Series **012092** https://doi.org/10.1088/1742-6596/1999/1/012092
16. R.Y. Hassan, A. S. Nadia, K. J. Alaa, Eurasian journal of mathematical and computer applications **8(4)**, 97-107 (2020) https://doi.org/10.32523/2306-6172-2020-8-4-97-107
17. A. Azizi, E.H. Laaji, Journal of Cyber Security and Mobility **11(5)**, 673-694 (2022) https://doi.org/10.13052/jcsm2245-1439.1152
18. C. Bonte, I. Ilyashenko, J. Park, H. Pereira, N. Smart, *FINAL: Faster FHE Instantiated with NTRU and LWE*. Advances in Cryptology ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, pp 185-215 (2022) https://doi.org/10.1007/978-3-031-22966-4_7
19. W. Dai, W. Whyte and Z. Zhang, IEEE Transactions on Computers **67(11)**, 1572-1583 (2018) https://doi.org/10.1109/TC.2018.2809723.
20. P. Kirchner, P. Fouque, Advances in Cryptology – EUROCRYPT 2017, Springer, Cham, **10210**, 3-26 (2017) https://doi.org/10.1007/978-3-319-56620-7_1
21. F. Wu, B. Zhou, X. Zhang, Entropy **25**, 454 (2023) https://doi.org/10.3390/e25030454
22. J. Sepulveda, A. Zankl and O. Mischke, *Cache attacks and countermeasures for NTRUEncrypt on MPSoCs: Post-quantum resistance for the IoT*. 30th IEEE International System-on-Chip Conference (SOCC), Munich, Germany, pp. 120-125 (2017) https://doi.org/10.1109/SOCC.2017.8226020
23. W. Dai, W. Whyte, Z. Zhang, IEEE Transactions on Computers **67(11)**, 1572-1583 (2018) https://doi.org/10.1109/TC.2018.2809723
24. S. Sánchez-Solano, E. Camacho-Ruiz, M.C. Martínez-Rodríguez, P. Brox, Sensors **22,** 2057 (2022) https://doi.org/10.3390/s22052057
25. Kim Taehyun, Mun-Kyu Lee, IEEE Access **8**, 126591-126605 (2020) https://doi.org/10.1109/ACCESS.2020.3008182
26. T. Fritzmann, T. Schamberger, C. Frisch, K. Braun, G. Maringer, M.J. Sepúlveda, *Efficient Hardware/Software Co-design for NTRU*. IEEE/IFIP International

Conference on Very Large Scale Integration of System-on-Chip, pp. 257-280 (2018) https://doi.org/10.1007/978-3-030-23425-6_13