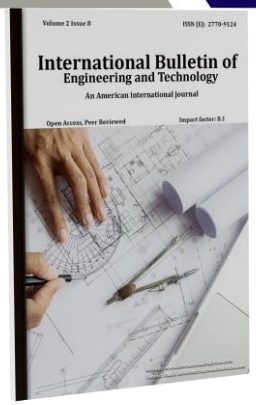

PHYSICAL FACILITIES OF INFORMATION SECURITY

D. Musakhanov
Turin Polytechnic University in Tashkent
Email: diyor.musakhanovv@gmail.com
A. Kudaibergenov
Kazakh-British Technical University
Email: kudaibergenov2a@gmail.com
https://doi.org/10.5281/zenodo.10171295

Abstract

In the age of digitalization, where information has evolved into a critical asset, safeguarding data and preserving privacy have emerged as paramount concerns for both organizations and their personnel. The physical aspect of information protection assumes a pivotal role in thwarting unauthorized access to sensitive data and vital infrastructure. This paper endeavors to examine the current methodologies, technologies, and strategies employed to guarantee the physical security of information.

Keywords: security, information, data security, technologies.

INTRODUCTION

In the age of digital advancements, the Information Technology (IT) sector is experiencing exponential growth and transformation. This rapid evolution has opened up new horizons of possibilities, enabling organizations to streamline operations and provide innovative services. However, with these technological advancements come significant challenges, one of the most pressing being the potential for information leakage and security breaches. In today's interconnected world, where data has become a currency of its own, the security of information sources is paramount. Organizations across sectors, including financial institutions, corporations, and government entities, find themselves in the crosshairs of cyber threats and information vulnerabilities. To effectively combat these risks, a multifaceted approach to safeguarding information is imperative.

While information security comprises various facets such as organizational policies, software, and hardware protections, the focus of this paper rests squarely on the physical aspect of information security. This dimension involves tangible, real-world measures that act as a bulwark against unauthorized access, theft, or tampering of information sources. It's important to note that physical security is just one piece of the larger puzzle known as engineering and technical protection of information, which encompasses a broader spectrum of security measures.

Theoretical Background

Information security is a multifaceted discipline dedicated to protecting information and information systems from an array of threats, including unauthorized access, unauthorized use, data disclosure, system disruption, data modification, and data destruction. Its overarching goals are to ensure data integrity, confidentiality, and availability.

Engineering and technical protection of information extends beyond the digital realm to include physical safeguards. This holistic approach encompasses strategies like securing physical infrastructure, concealing sensitive information, and neutralizing potential threats stemming from physical sources.

The organizational facet of information security encompasses the legal and regulatory framework governing data protection. It encompasses the development and enforcement of legislation, laws, and rules, both at the governmental and organizational levels.

Software and hardware protection focuses on implementing a range of measures to secure information within computer systems and networks. These measures help thwart unauthorized access, ensuring data remains confidential and secure.

Physical protection of information, as defined here, involves a comprehensive set of measures designed to increase the time, effort, and resources required for potential adversaries to access critical information sources. This serves as a crucial barrier against unauthorized intrusions and data breaches.

Cyber-Physical Systems (CPS) represent a significant technological advancement that seamlessly integrates digital and physical components. Leveraging cutting-edge sensor technology, computing capabilities, and network connectivity, CPS enable more efficient and interconnected systems that can benefit a wide range of industries.

Physical Security and Information Security: An Interconnected Paradigm

The foundational principles of physical security serve as the bedrock for safeguarding information assets. Literature in this domain elucidates the importance of securing physical access points, surveillance systems, and environmental controls (Vacca, 2013; Whitman & Mattord, 2018). This includes considerations for perimeter security, access control mechanisms, and surveillance technologies that contribute to the overall protection of information assets.

Scholars have explored how physical security measures act as critical components in risk mitigation strategies. This includes studies on the implementation of access control systems, surveillance cameras, and intrusion detection systems to mitigate unauthorized physical access (Peltier, 2013; Easttom, 2018). The literature delves into the effectiveness of these strategies in reducing the likelihood of physical breaches and their impact on overall information security.

The convergence of physical and cybersecurity has gained prominence in recent literature. Research emphasizes the need for an integrated approach, where physical security measures seamlessly align with cybersecurity protocols (Vacca, 2013; Kizza, 2019). This involves analyzing how physical breaches could lead to cyber threats and vice versa, necessitating a holistic security strategy that bridges the physical-cyber gap.

Studies delve into the integration of biometric technologies as part of physical access control measures. Biometric systems, including fingerprint scanners and facial recognition, are explored for their efficacy in enhancing physical security (Nellis et al., 2016; Jain et al., 2020). The literature discusses the strengths and vulnerabilities of biometric technologies and their role in bolstering information security.

The literature explores the implications of smart building technologies and the Internet of Things (IoT) on information security within physical spaces (Zheng et al., 2017; Hong et al., 2018). This includes discussions on securing interconnected devices, sensors, and systems to prevent potential vulnerabilities that may be exploited for cyber-physical attacks.

Recent studies delve into the application of blockchain technology for enhancing the physical security of information assets (Conti et al., 2018; Al Omar et al., 2020). The literature discusses how blockchain can provide immutable and decentralized solutions for securing physical access logs, surveillance data, and other critical components of physical security infrastructure.

This literature review provides a comprehensive overview of the evolving landscape of physical facilities in information security. As organizations navigate the complexities of securing their information assets, the integration of robust physical security measures emerges as an indispensable aspect of a holistic security strategy. The synthesis of current research underscores the need for organizations to consider both physical and cyber dimensions in their quest to fortify information security frameworks. Moving forward, continued exploration and innovation in the intersection of physical and cybersecurity realms will be pivotal for adapting to emerging threats in an increasingly interconnected world.

ANALYSIS AND RESULTS

To begin with, it is important to know that physical security is a first milestone for any attacker trying to gain access to confidential information, therefore, its importance cannot be questioned.

Physical security must include protection from unauthorized modification, deletion and interception of information. Moreover, accessibility and confidentiality must be ensured for authorized users. It is also necessary that the information is not exposed to threats associated with safe storage. Overall, the physical part of information protection must correspond to the CIA triad model.

The main arsenal for providing physical protection are including:

- Fencing and physical isolation systems
- Physical Access Control Systems (PACS)
- Locking devices and lockers
- Electronic and physical counterintelligence devices

Fencing and physical isolation systems

Fencing and physical isolation systems must ensure security on the perimeter of the area, security of the buildings and their elements inside. The examples of elements of such systems are sensors, walls, windows, window bars, cabinets, doors. Usually, such elements have an approximate time required to overcome them.

Table 1. Examples of the time it takes a skilled attacker to overcome obstacles.

Type of an obstacle and its parameters	Time to overcome (s)
Window, glass thickness - 4 mm	9-12
Window with metal bars (bar d = 20 mm)	150-170
Wooden door	12-15

Wooden door covered with iron	90-110
Metal door with bars (bar d = 20 mm)	120-150
The door made of solid metall (sheet thickness - 4 mm)	300-400
Brick wall, thickness - 30 cm	400-450
Cabinet with metal walls, thickness 2 mm	70-90

Source: Developed by the author

Based on this, some obvious measures are also proposed:

1. Create additional obstacles on the highest likely routes of the attacker to prevent an attacker's access to the information source.
2. Ensure a clearly visible area on the most likely attack routes.
3. Set up modern sensors for fire detection and automatic fire extinguishing, because usually, fire is the second most possible threat.

Therefore, the time necessary for attacker to overcome the path to information source can be described as:

$$\tau_a = \tau_m + \sum_{i=0}^{n} \tau_i$$

Where τ_m – attacker's movement time and τ_i – time to overcome an obstacle.

According to this, the well functioning system of objects of physical protection must satisfy this conditions:

$$\tau_o = \Delta + \tau_n + \tau_d$$

$\delta < \tau_a$ & $\tau_d < \tau_a$

Where δ – delay between detection and neutralization, τ_n – neutralization time and τ_d – detection time.

It is assumed that when neutralization begins, the attacker stops their movement, otherwise, inequality changes as

$\tau_o < \tau_a$

Where τ_a - attacker's speed on the path to the information source, τ_o - complex of measures for detecting and neutralizing an attacker.

Physical Access Control Systems (PACS)

Physical Access Control Systems - complex of technical and software measures aimed to manage entry and exit of objects through "Passage points" such as doors, gates and checkpoints. These include RFID cards, digital keys, biometric authentication, smart locks and time based access.

Such systems are a great decision to deny access for private information for unauthorized individuals. However, this solution must be set up correctly and to avoid uncertainties must satisfy some conditions.

Firstly, unambiguous identification must be present in each type of authentication method. Secondly, the rights of users must be set up regarding their positions. For example, an accountant does not need access to a server room where confidential information circulates. Finally, these systems must be protected from internal influence. For instance, if a

digital lock is attacked with electromagnetic impulses (EMI), it must contain a protection mechanism that will give a signal to the security service before it breaks down.

In general, PACS must satisfy these key conditions: Functionality, robustness, security and they should be easy to use. Functionality must include such opportunities as unambiguous authentication and authorisation and audit with logging on each node of a system. Robustness must ensure fault tolerance at any time. Thus, there should be backup power supplies which are connected to the PACS. From the security point of view all critical credentials must be stored and distributed in an encrypted way. Finally, the system must be scalable and protected from physical threats.

Locking devices and lockers

Locking devices and lockers play a crucial role in ensuring protection in the information system. Usually, it is the final milestone with which an attacker encounters on the path to steal information. It is a well known fact that lockers must be protected from external influence, including different weather conditions. Moreover, on the example of ordinary lockers they must have protection from lock picking, bumping, drilling, breaking, etc.

The authentication and identification must be reliable, use securely protected keys which cannot be counterfeited or copied illegally. Key management should be organized, each issue and withdrawal of a key must be recorded along with the time and ID of a person who used it.

The critical information objects such as servers which store valuable information must be strongly protected, because the fall of this milestone means the fall of the entire system of defense. The use of armored safes and cabinets with various additional functions for critical information system objects is an integral part of the correct provision of security. In addition, these functions can isolate systems from dust, excess moisture, and have embedded fire extinguishing, cooling, protection from electromagnetic rays and backup power systems.

Electronic and physical counterintelligence devices

Electronic counterintelligence devices are designed to detect and prevent eavesdropping of information and data interception attempts.

First of all, it is necessary to ensure the protection of information from surveillance and eavesdropping. For example, to prevent leakage along an optical channel, energy hiding methods are used by increasing the attenuation of the propagation medium. Tools and methods that are used include window tinting, blinds and automatic door closers, and regular testing for radio-emitting spying devices should be carried out using devices such as field indicators, automated radio monitoring systems, non-linear locators and metal detectors. Protection against eavesdropping of speech information is also equally important. These include increasing sound insulation, using thicker walls and doors, and using acoustic jammers. In fact, there are an innumerable number of methods of electronic information theft and protection against them. All of them, of course, cannot be listed within one work, so only the most common ones will be considered. Basic methods of prevention include turning off all unnecessary radio-electronic devices, installing suppressors of acoustoelectric converters, devices preventing low-frequency imposition, spatial electromagnetic noise generators, and installing a noise generator in a free slot on the computer motherboard. A Faraday cage is an example of a device that is used to block electromagnetic signals and ensure the confidentiality of information that is contained within the protected space.

CONCLUSION

To summarize, this article reviewed existing and used methods related to issues of ensuring the physical protection of information. It is worth noting that many of the physical methods discussed should be used in conjunction with software and organizational solutions to ensure comprehensive information protection. With the growth of threats to information security, it is necessary to keep up with the times and improve algorithms for ensuring complex information protection, conduct more research on this topic and educate individuals, even if they are not related to this sphere.

References:

1. NIST SP 800-59 under Information Security from 44 U.S.C., Sec. 3542 (b)(1), URL:
2. https://www.govinfo.gov/app/details/USCODE-2008-title44/USCODE-2008-title44-chap35-subchapII-sec3542
3. Torokin A.A., 2005. Engineering and technical protection of information. ISBN 5-85438-140-0., URL: https://search.rsl.ru/ru/record/01002805947
4. Dolgiy P.A., Kosterev M.S., Sushkov A.E., Pylinskaya Y.A., Gudkov V.V. Current issues of physical information protection, URL: https://cyberleninka.ru/article/n/aktualnye-voprosy-fizicheskoy-zaschity-informatsii/pdf
5. Burkova E.V., 2017, Physical protection of informatization objects, URL: http://elib.osu.ru/bitstream/123456789/13741/1/36384_20170503.pdf
6. Arunesh Sinha, Thanh H. Nguyen, Debarun Kar, Albert Xin Jiang, Milind Tambe, Matthew Brown. "From physical security to cybersecurity." November 2015. Journal of Cybersecurity 1(1). DOI: 10.1093/cybsec/tyv007. License: CC BY-NC-ND 4.0., URL: https://www.researchgate.net/publication/284161432_From_physical_security_to_cybersecurity
7. NIST SP 1800-2, NIST SP 1800-2b, NIST SP 1800-2c, NIST SP 800-161r1, NIST SP 800-73-4, Physical Access Control System, URL: https://csrc.nist.gov/glossary/term/physical_access_control_system
8. Abidarova A.A., Physical information security measures, URL: https://cyberleninka.ru/article/n/fizicheskie-sredstva-zaschity-informatsii/viewer
9. Wikipedia, Physical information security, URL: https://en.wikipedia.org/wiki/Physical_information_security
I.Begishev, A. Bokovnya., 2022, Architecture Of Information Security Threats in Cyber-Physical Systems. URL: https://www.researchgate.net/publication/366685586_Architecture_Of_Information_Security_Threats_in_Cyber-Physical_Systems
10. Al Omar, A., Basu, A., & El Khatib, K. (2020). Securing the Internet of Things using Blockchain technology. Computers & Security, 88, 101614.
11. Conti, M., Kumar, E., Lal, C., Ruj, S., & Sandhu, R. (2018). A survey on security and privacy issues of blockchain technology. IEEE Communications Surveys & Tutorials, 20(4), 3684-3715.
12. Easttom, C. (2018). System Forensics, Investigation, and Response. Nelson Education.
13. Hong, K., Kim, D., Kim, H., & Lee, S. G. (2018). A survey of the Internet of Things (IoT) in healthcare: Security and privacy issues. Journal of Information Processing Systems, 14(1), 101-112.

14. Jain, A. K., Dass, S. C., & Nandakumar, K. (2020). Biometric Authentication: A Machine Learning Approach. Springer.
15. Kizza, J. M. (2019). Guide to Computer Network Security. Springer.
16. Nellis, J. C., Meyer, J., & O'Daniel, M. (2016). Biometric and Surveillance Technology for Human and Activity Identification. IGI Global.
17. Peltier, T. R. (2013). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press.
18. Vacca, J. R. (2013). Computer and Information Security Handbook. Morgan Kaufmann.
19. Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security. Cengage Learning.
20. Zheng, Y., Capossele, A., Zheng, Y., & Shen, H. (2017). Cyber–physical attack and defense in the Internet of Things. IEEE Internet of Things Journal, 4(6), 1910-1920.