УДК 004.056.53

PROTECTION AGAINST UNAUTHORIZED ACCESS

Tetiana Laptieva

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Тетяна Лаптєва

State University of Trade and Economics / Kyiv National University of Trade and Economics, Kyoto St., 19, Kyiv, 02156, Україна

Abstract*. This paper explores modern methods for securing information systems against unauthorized access. As cyber threats grow, ensuring data confidentiality, integrity, and availability is essential. The study highlights the need for a comprehensive security strategy combining organizational policies, technical controls, and advanced software. It addresses challenges in cloud environments and the use of AI for anomaly detection. Legal frameworks like GDPR and national standards are also examined. Effective protection requires continuous monitoring, strong access controls, and proactive threat response. Multi-layered defenses—such as encryption, two-factor authentication, and behavioral analytics – improve resilience against both internal and external threats.*

In the context of rapid growth in cyber threats and the digital transformation of all spheres of societal life, ensuring information system security has become increasingly important. One of the key areas of information security is protection against unauthorized access (PUA), which involves preventing illegal acquisition, modification, or destruction of data. The necessity for effective countermeasures against unauthorized access is driven both by the increasing number of cyberattacks and the growing volume of confidential information stored and processed digitally.

Unauthorized access refers to any acquisition of data, system resources, or administrative privileges without prior permission from the data owner or the respective security authority. Such access can be accidental or intentional, technical or organizational, internal (from employees) or external (from hackers). The most common methods of unauthorized access include: use of weak passwords; phishing attacks; SQL injections; exploitation of vulnerabilities in operating systems and software; social engineering; and the use of malicious software (viruses, Trojans, ransomware).

Methods and Tools for Counteracting Unauthorized Access

An effective protection system against unauthorized access must be comprehensive and multi-layered. The main directions of defense include:

Organizational measures : development and implementation of a security policy; granting users only the minimum necessary access rights (principle of least privilege); conducting regular access audits; and training personnel in information security.

Technical tools: firewalls and intrusion detection/prevention systems (IDS/IPS); data encryption (disk-level, database, and network protocol encryption); two-factor authentication (2FA); role-based access control (RBAC); endpoint security and protection of network entry points.

Software mechanisms : implementation of identity and access management systems (IAM); event log analysis (SIEM); antivirus and anti-spyware software; and regular software updates to patch vulnerabilities.

Specifics of Protection in Cloud Environments

The development of cloud services and remote data storage technologies introduces new challenges in the field of unauthorized access prevention. Key risks include loss of control over physical resources, abuse of cloud administrator privileges, misconfiguration of cloud services, and cross-exposure of client data. To minimize these threats, specific countermeasures should be implemented, such as data encryption before uploading to the cloud, adoption of zero-trust

architectures, regular audits of cloud service configurations, API access control, and the use of Cloud Access Security Brokers (CASB).

Artificial Intelligence in Systems for Protecting Against Unauthorized Access

Data analysis based on machine learning and artificial intelligence is increasingly used to detect anomalies in user and system behavior. AI technologies enable automatic identification of suspicious activity, prediction of potential attacks, and real-time threat response. A notable approach is User and Entity Behavior Analytics (UEBA), which analyzes the behavior of users and other entities within the system to identify deviations from normal patterns that may indicate unauthorized access.

Legal Framework for Protection Against Unauthorized Access

The legal aspect is equally important. Many countries have enacted laws regulating information security, including: the General Data Protection Regulation (GDPR, EU) – for personal data protection; NIST Cybersecurity Framework (USA); the Law of Ukraine "On Personal Data Protection"; and national information security standards (DSTU, GOST, etc.). Non-compliance may lead to significant penalties, reputational damage, and loss of user trust.

Conclusion

Ensuring the security of information systems against unauthorized access is a core element of modern cybersecurity. As cyber threats grow in scale and complexity, protecting data confidentiality, integrity, and availability has become essential. Common attack vectors include weak passwords, phishing, SQL injections, software vulnerabilities, social engineering, and malware. To counter these risks effectively, a comprehensive and multi-layered strategy is required.

Organizational measures such as developing clear security policies, applying the principle of least privilege, conducting regular access audits, and training staff are crucial. Since human error remains a major vulnerability, fostering a strong security culture is vital.

Technical tools like firewalls, intrusion detection and prevention systems (IDS/IPS), encryption, two-factor authentication, role-based access control (RBAC), and endpoint protection form the backbone of cyber defense. These tools help prevent breaches and protect sensitive data.

Software solutions including identity and access management (IAM), SIEM for real-time monitoring, antivirus programs, and timely patching of vulnerabilities enhance system resilience. Proactive maintenance significantly lowers the risk of exploitation.

Cloud environments bring new challenges such as misconfigurations, excessive privileges, and data exposure. Effective countermeasures include encrypting data before upload, adopting zero-trust architecture, controlling API access, and using Cloud Access Security Brokers (CASB).

Artificial intelligence and machine learning increasingly support threat detection. User and Entity Behavior Analytics (UEBA) enables real-time identification of anomalies and is especially useful for detecting insider threats.

Legal compliance with frameworks like GDPR, NIST Cybersecurity Framework, Ukrainian Personal Data Protection Law, and national standards (DSTU, GOST) is also essential. Non-compliance can lead to penalties, reputational damage, and loss of user trust.

In conclusion, robust protection requires a combination of organizational policies, technical controls, advanced software, and legal compliance. Future progress lies in adopting emerging technologies such as AI, blockchain, and zero-trust models. Only through a systemic and integrated approach can real information security be achieved in today’s digital world.

Reference

1. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others. Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c. ISBN 978-617-7319-31-2 (on-line). ISBN 978-617-7319-32-9 (print). DOI: https://doi.org/10.15587/978-617-7319-31-2
2. Laptiev O., and other. Methodological aspect of ensuring state security in the mind threats. University of Security Management in Koshitze. Slovakia. 2023. 272 p. ISBN 978-80-8185-058-5. (Charter 10. pp.137-150).