UDC 004.056:336.71(076)

TECHNICAL MEANS OF INFORMATION PROTECTION

Zihan Huang
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article discusses modern technical means of information protection, including hardware and software-hardware complexes. A classification is provided, along with the operating principles and examples of implementing systems designed to counter unauthorized access, technical channel leakage, and malicious impacts. A method for personal data protection based on the identifiers introducing is proposed, which enhances the security of identification and authentication processes. Special attention is paid to the certification and effectiveness of applying such means in critical information systems.
Keywords: technical information protection; information security means; unauthorized access; firewalls; intrusion detection system; cryptographic gateway; biometric

authentication; identifiers introducing; personal data protection; security tools certification; information leakage; malware protection.

Introduction

The current stage of development of the information society is characterized by the growing role of information as a key strategic resource. At the same time, the number of threats aimed at violating the confidentiality, integrity, and availability of information is increasing. Technical means of information protection play a central role in building a comprehensive information security system. They include a wide range of devices, systems, and complexes designed to protect information processed, stored, and transmitted in automated systems. The relevance of this topic is confirmed by the steady growth of cyberattacks, the complexity of modern malicious software, and the tightening of regulatory requirements for information protection in critical infrastructure facilities. The purpose of this work is to analyze the current state, classification, and features of the application of technical means of information protection, with a focus on modern methods for personal data protection based on identifiers introducing.

Main Part

Modern technical means of information protection can be classified according to their functional purpose, method of implementation, and level of protection provided. Based on their functional purpose, the following main classes are distinguished: means of protection against unauthorized access, means of protecting against information leakage through technical channels, means of cryptographic information protection, and means of security monitoring and analysis.

An example of the figure design and the caption to it is presented below. Figure shows a generalized structural diagram of interaction between various technical means of information protection within a corporate information system.

Among the promising approaches to enhancing personal data security, the method based on identifiers introducing deserves special attention. This method involves the generation and assignment of unique identifiers to data subjects and their personal data attributes, enabling fine-grained access control and traceability. The core principle is to replace direct personal identifiers with derived identifiers that are used throughout the system, thereby reducing the risk of unauthorized correlation and disclosure.

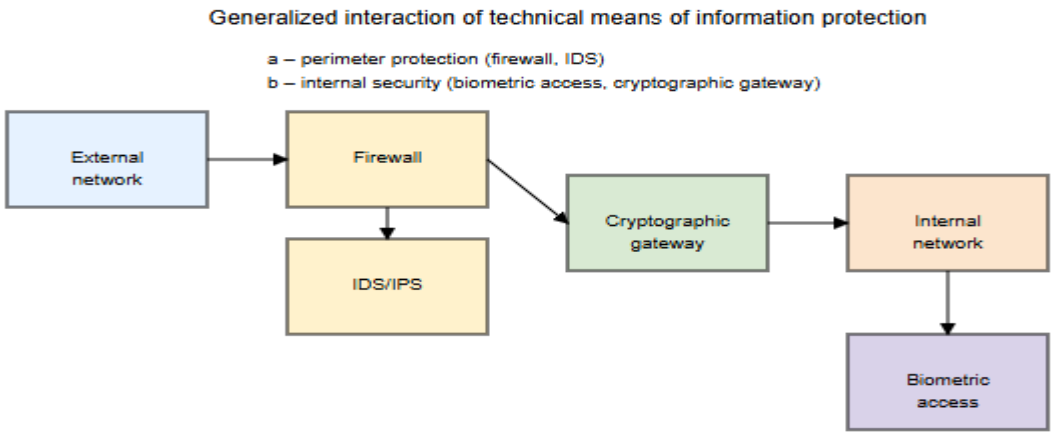

Figure capture: a – perimeter protection (firewall, intrusion detection system); b – internal security (biometric access control, cryptographic gateway)

The effectiveness of the identifiers introducing method can be evaluated by the reduction in the probability of successful re-identification. The probability that an attacker successfully links a set of actions to a specific data subject is given by:

$$P\_reid = P\_initial * (1 - R\_id), \quad (1)$$

where P_reid – the probability of successful re-identification; P_initial – the probability of re-identification without identifier transformation; R_id – the reduction coefficient achieved through identifier introducing ($0 \leq R\_id \leq 1$). As R_id approaches 1, the risk of re-identification approaches zero.

Examples of equation design are provided below. To assess the effectiveness of technical protection means, one can use the probability of overcoming protection as a key indicator. The total probability of unauthorized access when sequentially overcoming n protection lines is determined by the formula:

$$P\_total = 1 - \prod\_\{i = 1\}\^\{n\} (1 - P\_i), \quad (2)$$

where P_total – the total probability of unauthorized access; P_i – the probability of overcoming the i-th line of defense; n – the number of lines of defense. This expression demonstrates that increasing the number of independent lines of defense significantly reduces the overall probability of a successful attack.

An example of table design is presented below. A comparative analysis of the main technical means of information protection is provided in Table including the identifiers introducing method as a supplementary control.

Comparative characteristics of technical means of information protection

Type of means	Function	Implementation	Certification requirement
Firewall	Network traffic filtering	Hardware and software	Mandatory
Intrusion detection system	Attack detection	Software and hardware	Mandatory
Cryptographic gateway	Data encryption	Hardware and software	Mandatory
Biometric authentication	Identity verification	Hardware and software	For critical systems
Identifiers introducing method	Personal data protection, traceability	Software	Recommended for personal data systems
Security scanner	Vulnerability assessment	Software	Recommended

Conclusion

Technical means of information protection are a key element of modern information security systems. The analysis showed that the most effective is a comprehensive approach combining perimeter protection tools, cryptographic protection, biometric access control systems, and advanced methods for personal data protection such as the identifiers introducing method. The identifiers introducing method provides enhanced protection for personal data by substituting direct identifiers with derived ones, significantly reducing the risk of re-identification and unauthorized access. A promising direction for further development is the integration of artificial intelligence methods for behavioral analysis of users and detecting anomalies, as well as the transition to import-independent technical protection means in critical sectors. The development and implementation of effective technical protection means require constant updating of approaches in accordance with the dynamics of threats.

References

1. Comprehensive Approach to Designing Technical Information Protection Systems
2. Modern Intrusion Detection Systems: Architectures and Effectiveness
3. Guidelines on Certification of Technical Information Protection Means
4. Application of Cryptographic Gateways in Corporate Networks
5. Dynamic Identifier-Based Protection Framework for Personal Data in Distributed Systems
6. Methods of Making Management Decisions

Information about the author

Zihan Huang, master student of Educational Institution "Belarusian State University of Informatics and Radioelectronics", e-mail: 1913017013@qq.com.