COMPUTER SYSTEMS SECURITY

(Textbook for Universities and Colleges)

AUTHORS

Masimov Afiq Gazanfar
Mammadov Mahil Isa
Mammadov Mahmud Neyman
Orudjova Mehseti Uzevir
Taghiyeva Yegana Hikmat
Baratzade Naciba Zulfigar

COMPUTER SYSTEM SECURITY

(Textbook for Universities and Colleges)

NEX GEN PUBLICATIONS

India | UAE | Nigeria | Uzbekistan | Montenegro | Iraq | Egypt | Thailand | Uganda | Philippines | Indonesia

www.nexgenpublication.com

COMPUTER SYSTEM SECURITY

(Textbook for Universities and Colleges)

Authored By:

Masimov Afiq Gazanfar
Associate Professor, Department of Information Technologies, Azerbaijan State Agricultural University

Mammadov Mahil Isa
PhD in Engineering, Associate Professor, Department of Information Technologies, Azerbaijan State Agricultural University

Mammadov Mahmud Neyman
Associate Professor, Department of Information Technologies, Azerbaijan State Agricultural University

Orudjova Mehseti Uzevir
Associate Professor, Department of Information Technologies, Azerbaijan State Agricultural University

Taghiyeva Yegana Hikmat
Senior Lecturer, Department of Information Technologies, Azerbaijan State Agricultural University

Baratzade Naciba Zulfigar
Senior Lecturer, Department of Information Technologies, Azerbaijan State Agricultural University

First Impression: August 2026

COMPUTER SYSTEM SECURITY

(Textbook for Universities and Colleges)

ISBN: 978-81-69295-20-8

Rs. 1000/- ($80)

DOI: https://doi.org/10.5281/zenodo.22106903

Total Pages: 493

Published by:
Nex Gen Publications

UDC: 004.056(075.8)
BBK: 32.973-018я73
LCC: QA76.9.A25 M37 2026
DDC: 005.8
Author mark: M37

Afiq Masimov, Mahil Mammadov, Mahmud Mammadov, Mehseti Orudjova, Yegana Taghiyeva, Baratzade Naciba. Computer Systems Security. (Textbook for universities and colleges). - pp.

This textbook establishes the core concepts and definitions of information security, while analyzing threats to information security in computer systems. It defines the fundamental principles of security policies and reviews key cryptographic methods and algorithms used for protecting information in computer environments.
Furthermore, the book justifies a comprehensive approach to ensuring information security in enterprise networks and describes the primary technologies for securing internetwork data exchange. Antivirus protection methods and tools are also thoroughly examined. Additionally, the organizational and legal framework of information security is outlined based on international standards and guidelines.
The textbook is specifically designed for undergraduate (Bachelor's) students majoring in Computer Engineering. It is also an invaluable resource for students pursuing degrees in Information Technology and Information Security, as well as for IT professionals and security specialists.

Preface

The rapid development of digital technologies, computer networks, cloud services, electronic communication platforms and automated information systems has significantly changed the structure of modern society, education, science, production and management. Today, information is not only a technical resource, but also a strategic asset that determines the stability, efficiency and competitiveness of institutions, enterprises and individuals. Therefore, the protection of information, the reliable operation of computer systems and the prevention of unauthorized access have become one of the most important tasks of modern information technologies.

Computer system security is a multidisciplinary field. It combines theoretical concepts, technical mechanisms, organizational measures, legal requirements and practical protection methods. The effective protection of information resources requires a systematic understanding of confidentiality, integrity, availability, authentication, authorization, access control, cryptographic protection, network security, malware prevention, risk analysis and security policy. For this reason, the study of computer system security is essential for students, researchers and specialists working in the fields of computer engineering, information technologies and information security.

This textbook, Computer Systems Security, has been prepared to provide students with a structured and academically grounded understanding of the main principles, methods and technologies used in the protection of computer systems and networks. The book explains the fundamental concepts of information security, analyzes the main types of threats to computer systems, presents the principles of security policy, and discusses the basic cryptographic methods and algorithms used for information protection. Special attention is given to the security of corporate networks, protected data exchange between networks, firewall technologies, virtual private networks, antivirus protection, intrusion detection, access control and the organizational and legal foundations of information security.

The content of the textbook is designed to combine theoretical knowledge with practical relevance. The material is arranged in a logical sequence so that the reader can first understand the basic concepts of information security

and then gradually move toward more complex topics related to network protection, cryptographic mechanisms, corporate security architecture and security management. This approach makes it possible to form not only technical knowledge, but also analytical thinking about risks, vulnerabilities and protection strategies.

The textbook is primarily intended for undergraduate students majoring in Computer Engineering. At the same time, it may be useful for students of information technologies, information security and related specialties, as well as for specialists who deal with the design, operation and protection of computer systems and networks. The book can also serve as a methodological resource for teachers, researchers and practitioners interested in the development of secure information infrastructures.

In preparing this textbook, the authors aimed to present the material in a clear, consistent and academically appropriate form. The explanations are based on generally accepted concepts, open scientific and technical sources, standards and practical approaches used in the field of information security. The purpose of the book is not only to describe existing security technologies, but also to help readers understand the logic of building reliable, scalable and manageable protection systems.

The authors express their hope that this textbook will contribute to the development of professional knowledge in the field of computer system security and will support the training of qualified specialists capable of responding to modern cybersecurity challenges. The authors will be grateful for comments, suggestions and recommendations that may help improve future editions of the textbook.

The Authors Respectfully,
The Authors

Introduction

The Internet is a technology that has produced fundamental transformation across the principal domains of human activity. It has altered the pace of scientific progress, the direction of technological development, and the character of the working environment. Communication models have become an integral component of this transformation.

Effective use of information technology constitutes one of the strategic conditions that determine an enterprise's competitive capacity. Here, the central issue extends beyond mere technology deployment. An enterprise must align such technology with the logic of management, communication, and security.

Development of an enterprise information system depends on numerous connections established through the Internet. These connections encompass diverse partners, remote users, service channels, and internal divisions. As communication expands, security requirements acquire a more stringent character.

Joint deployment of Internet, intranet, and extranet environments further complicates information security considerations. The boundary between the open network and the internal corporate environment weakens. Security policy must reconstruct this boundary at the technical, organizational, and legal levels.

Protection of the information security of corporate information systems is generally carried out through an information security system. Here, the term Corporate Information System is denoted by the abbreviation CIS. The term Information Security System is denoted in subsequent sections by the abbreviation ISS.

The principal requirement in building an ISS is protection of investments already directed toward the CIS. Security mechanisms must not disrupt the operation of existing software. They must function transparently for applications running within the CIS.

Transparency does not mean that the security mechanism remains invisible. This concept relates to preservation of applications' normal operating mode. The ISS must monitor, track risks, and restrict unauthorized activity without interfering with normal operation.

Full compatibility with the network technologies used within the CIS should be evaluated as a separate requirement. Where compatibility proves weak,

security tools may reduce system productivity. In more severe cases, such tools may disrupt the continuity of business processes.

An ISS designed for an enterprise must account for emerging technologies and services. The security architecture should not be confined to present needs alone. It must be built to withstand future expansion, evolving services, and growth in the number of users.

Every element of the CIS must rest on open standards, integrated solutions, and a scalable structure. These three requirements cannot function in isolation from one another. Open standards increase compatibility, integration simplifies management, and scalability extends the technical limits of growth.

Transition to open standards represents one of the principal directions in the development of information security tools. This choice reduces the risk associated with closed solutions tied to a single vendor. Compatibility problems arise less frequently when an enterprise modifies or expands its security tools.

Internet Protocol Security is denoted by the abbreviation IPsec. IPsec constitutes a set of protocols for protecting data transmitted through the IP protocol. This standard supports confidentiality, integrity, and authentication requirements across open communication channels.

Public Key Infrastructure is denoted by the abbreviation PKI. PKI rests on management of digital certificates, keys, and a chain of trust. In inter-enterprise electronic communication, this infrastructure forms the principal technical basis for reliable identification.

IPsec and PKI serve the secure establishment of external communication between enterprises. They also support compatibility with products used by partner enterprises and remote clients. This compatibility constitutes an essential technical condition for secure collaboration within a corporate environment.

X.509 digital certificates remain one of the baseline standards for authenticating users and devices. The certificate model confirms the identity of a user or device on a cryptographic basis. This mechanism reduces the risk of basing trust on passwords alone.

Security solutions designed with future development in view must support the IPsec, PKI, and X.509 standards. A solution that does not rest on such standards may create integration difficulties later. An enterprise should assess this risk during the design phase.

The concept of an integrated solution covers two principal directions. The first direction concerns coordination of security tools with other network elements. This includes the operating system, routers, directory services, and policy servers.

The term Operating System is denoted, upon first use, by the abbreviation OS. Quality of Service is expressed by the abbreviation QoS. QoS policy servers are used for prioritizing network resources and managing service levels.

The second direction concerns combination of diverse security technologies within a unified protective environment. This structure protects an enterprise's information resources through a coordinated mechanism rather than separate tools. Control operates more consistently once distinct technologies are subordinated to a single policy.

Combination of a firewall, a virtual private network gateway, and an IP address translator illustrates this principle. Virtual Private Network is denoted by the abbreviation VPN. Such integration protects traffic transmitted over an open channel and centralizes access rules.

As the CIS grows, the ISS must change in accordance with that growth. Here, the central issue extends beyond installing additional devices and software. The security system must preserve its integrity, manageability, and control logic.

Scalability is the technical property that allows gradual expansion of security tools. This property assists in achieving an optimal balance between cost and reliability. An enterprise first establishes the necessary level, then expands the system according to need.

In enterprises with numerous branches, scalability becomes a more demanding requirement. Dozens of partners, hundreds of remote employees, and millions of potential customers increase the security load. Communication efficiency declines when the ISS fails to manage this load.

Reliable protection of CIS resources requires application of advanced information security technologies within the ISS. These technologies do not substitute for one another. They cover distinct risk areas through complementary mechanisms.

Cryptographic protection is applied to preserve the confidentiality, integrity, and authenticity of data. Confidentiality prevents unauthorized persons from reading information. Integrity indicates that data have not been altered. Authenticity confirms that the source is reliable.

Authentication technologies verify the identity of users and network objects. This verification should not remain confined to a simple password mechanism. Reliable authentication can be reinforced through multi-factor, certificate-based, and context-oriented mechanisms.

Firewall technologies protect the corporate network from external threats originating in public communication networks. They control traffic on the basis of defined rules. These rules distinguish permitted, suspicious, and prohibited connections.

Virtual secure channel and VPN technologies protect data transmitted within an open communication environment. These technologies form a logically protected channel between remote users and the corporate network. The outcome is a more reliable model of remote access.

Guaranteed identification of the user is reinforced through tokens and other authentication devices. Tokens include smart cards, sensor memory devices, and Universal Serial Bus keys. Universal Serial Bus is denoted, upon first use, by the abbreviation USB.

Access control at the user level aims to prevent unauthorized entry into information resources. Each user must act only within the scope of authority granted. A proper distribution of authority also reduces internal risks.

PKI-based key management governs the issuance, storage, renewal, and revocation of certificates. Without this management, the public key mechanism cannot operate reliably. Uncontrolled circulation of keys may become a weak point within the security architecture.

Intrusion Detection is applied to actively monitor the security condition of information resources. This technology identifies suspicious behavior, anomalous traffic, and possible indicators of attack. Early detection shortens the response time to an incident.

Antivirus technologies restrict the entry and spread of malicious software within a system. This protection should not remain confined to file scanning alone. Mail traffic, web links, removable devices, and executable files must likewise remain under control.

Centralized management of the ISS must rest on a unified enterprise security policy. A unified policy limits the emergence of divergent rules across different divisions. This management model strengthens consistency of control and traceability of decisions.

A comprehensive approach to information security requires rational combination of individual technologies. Cryptography, authentication,

access control, firewalls, VPN, intrusion detection, and antivirus mechanisms must operate together. Only under this condition does protection of the CIS avoid remaining a fragmented set of measures.

In constructing a security architecture, an enterprise should give preference to the interrelation of technical tools rather than their number. A robust ISS rests on the principles of compatibility, scalability, transparency, and centralized management. These principles form the principal technological foundation for the continuous operation of the CIS.

About the Authors

Masimov Afiq Gazanfar Was Born On 18.05.1963. In 1985, The Faculty Of Applied Mathematics Of Baku State University Finished 1985 - 1990, The City Of Ulanovsk, Russian Federation, "MARS" Scientific Research Institute, 1990-2000 Worked As A Factory, Workshop Chief. Azerbaijan From 2000 To 2017 Department Of Information Technologies Of The State Agrarian University Worked As A Teacher. Information Technologies At Azerbaijan State Agricultural University.In 2017, He Is An Associate Professor Informationtechnology In The Department Of Information Technology

Mammadov Mahil Isa— PhD in Engineering, Associate Professor. Born on May 1, 1966, in Agdam village, Tovuz district. In 1990, he graduated from the Azerbaijan Polytechnic Institute (now Azerbaijan Technical University) with a degree in Electronic Computing Machines. On September 20, 2013, he defended his dissertation on “Improvement of the technology for preparing information-software-based feed pellets” and was awarded the degree of Doctor of Philosophy in Engineering in the specialty 3102.01 – Agroengineering. In 2017, he received the academic title of Associate Professor in the Department of Information Technologies. 1990–1994: Engineer-programmer at the Azerbaijan Agricultural Institute. 1994–2009: Leading specialist-programmer at the Ganja branch of the Azerbaijan Joint-Stock Commercial Bank. 2009–2017: Lecturer and Senior Lecturer at the Department of Information Technologies, Azerbaijan State Agrarian University.2017–pr sent: Associate Professor at the same department.

Mammadov Mahmud Neyman Was Born on March 20, 1963. In 1985, At Baku State University He Graduated from The Faculty Of Applied Mathematics. 1985-1992 "Khazri" Transcaucasian Technological Installation in the Department, In the Positions of Engineer-Programmer and Software Tuning Engineer Has Worked. Since 1992, He Has Been Working in the Department Of Information Technologies at Azerbaijan State Agricultural University. In 2017, He Is an Associate Professor in the Department Of Information Technology.

Orudjova Mehseti Uzeyir was born on December 16, 1967.In 1989, she graduated with honors from the Faculty of Mechanization of the Azerbaijan State Agricultural University.She completed his postgraduate studies at this university in 1993.Since 2014, she has been an associate professor in the Department of Information Technologies.

Taghiyeva Yegana Hikmat - Senior Lecturer. Was born on September 4, 1991. In 2013 she completed her bachelor' s degree in "Informatics teacher" at Ganja State University, and in 2015, she completed her master's degree in "Software of Computer Systems and Networks" at Baku State University. From 2015-2025, she worked as an assistant teacher in the Department of Information Technologies at Azerbaijan State Agrarian University. Since July 5, 2025, she has been working as a senior lecturer in the same department.

Baratzade Naciba Zulfiqar - Senior Lecturer. Baratzade Naciba was born on December 31, 1954. In 1975, she graduated with a degree in Economics and Accounting from the Azerbaijan Agricultural Institute.From 1976 to 1990, he worked as an instructor-inspector at the Ganja City State Bank. Since 1992, he has been working as an assistant in the Department of Information Technologies at the Azerbaijan State Agrarian University, and since 2000, he has been serving as a senior lecturer.

Table of Contents

ABOUT THE AUTHORS:

Masimov Afiq Gazanfar
Associate Professor
Department of Information Technologies
Azerbaijan State Agricultural University

Mammadov Mahil Isa
PhD in Engineering
Associate Professor
Department of Information Technologies
Azerbaijan State Agricultural University

Mammadov Mahmud Neyman
Associate Professor
Department of Information Technologies
Azerbaijan State Agricultural University

Orudjova Mehseti Uzevir
Associate Professor
Department of Information Technologies
Azerbaijan State Agricultural University

Taghiyeva Yegana Hikmat
Senior Lecturer
Department of Information Technologies
Azerbaijan State Agricultural University

Baratzade Naciba Zulfigar
Senior Lecturer
Department of Information Technologies
Azerbaijan State Agricultural University

ISBN 978-81-69295-20-8

India | UAE | Nigeria | Uzbekistan | Malaysia | Montenegro | Iraq | Egypt | Thailand | Uganda | Philippines | Indonesia
Nex Gen Publications || www.nexgenpublication.com || info@nexgenpublication.com