

NATIONAL UNIVERSITY  
"YURI KONDRATYUK POLTAVA POLYTECHNIC"

---

DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGIES  
AND SYSTEMS

**Y.O. ZHYVYLO**

# CORPORATE SECURITY



**STUDY MANUAL**

**POLTAVA – 2025**

NATIONAL UNIVERSITY  
"YURI KONDRATYUK POLTAVA POLYTECHNIC"

---

DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGIES  
AND SYSTEMS

**Y.O. ZHYVYLO**

# **CORPORATE SECURITY**

STUDY MANUAL

POLTAVA – 2025

UDC 004.056.53

LBC 32.988-5

Reviewers:

**O.V. Shefer**, Doctor of Technical Sciences, Professor, Head of the Department of Automation, Electronics, and Telecommunications, Institute of Information Technologies and Robotics National University «Yuri Kondratyuk Poltava Polytechnic»;

**V.V. Vasiuta**, PhD of Technical Sciences, Associate Professor, Associate professor of the Department of Computer and Information Technologies and System, Institute of Information Technologies and Robotics National University «Yuri Kondratyuk Poltava Polytechnic».

**Corporate Security**: study manual / [Y.O. Zhyvylo]. – Poltava: National University “Yury Kondratyuk Poltava Polytechnic”, 2025. – 165 p.

*The textbook covers the program material for the training of students in the field of knowledge 12 “Information Technologies” in the specialties 122 - Computer Science, 123 - Computer Engineering, and 125 - Cybersecurity and Information Protection. The educational publication is based on materials from lectures, group, and practical sessions on the course “Corporate Security”, as well as from the courses “Cybersecurity”, “Information Protection”, “Information Protection in Infocommunication Systems”, “Fundamentals of Information and Cybersecurity”, and “Theory of Information Warfare”. The manual is intended for students studying in the specialty 12 of the field of knowledge “Information Technology”.*

*The developed manual is dedicated to studying the fundamentals of corporate security. It covers key areas such as risk management, protection of sensitive data, securing communication channels, and defending against both internal and external threats. The guide highlights the importance of implementing security policies, creating a robust security culture within an organization, and training employees to prevent social engineering attacks. Additionally, it emphasizes the significance of continuous monitoring, incident response, and the use of advanced security technologies to safeguard corporate infrastructure and information assets.*

Recommended for publication by the Scientific and Methodological Council of the National University “Yury Kondratyuk Poltava Polytechnic”  
Protocol №. 20 of February 2025

© Authors are listed on the back of the title page, 2025  
© Y.O. Zhyvylo 2025

## TABLE OF CONTENTS

	LIST OF ABBREVIATIONS	6
	INTRODUCTION	7
CHAPTER 1	INTRODUCTION TO CORPORATE SECURITY	8
	1.1. Definition of Corporate Security	8
	1.2. Main Threats and Risks in Corporate Environment	10
	1.3. The Role of Corporate Security in Business Processes	13
	1.4. The Importance of Confidentiality and Data Protection	15
CHAPTER 2	OVERVIEW OF CORPORATE SECURITY POLICIES AND STANDARDS	18
	2.1. Overview of Security Standards and Policies: ISO/IEC 27001, NIST	18
	2.2. Definition of Security Policies in an Organization	20
	2.3. Regulations and Laws on Information Protection	23
CHAPTER 3	SECURITY ARCHITECTURE IN CORPORATE SYSTEMS	27
	3.1. Types of Security Architectures: Perimeter, Multi-layered, Flexible	27
	3.2. The Role of Network Security	30
	3.3. Cloud Security in the Corporate Environment	33
CHAPTER 4	FUNDAMENTALS OF RISK MANAGEMENT IN CORPORATE SECURITY	37
	4.1. Risk Definition, Assessment, and Management	37
	4.2. Risk Mitigation and Adaptation Methods	39
	4.3. Implementation of Countermeasures to Minimize Risks	42
CHAPTER 5	DATA PROTECTION AND ACCESS MANAGEMENT	46
	5.1. Data Protection Methods	46
	5.2. Access Management Strategies	48
	5.3. The Importance of Authentication and Authorization	51
CHAPTER 6	INFORMATION SECURITY AND CYBERSECURITY	55
	6.1. Protection Against Cyber Threats (Attacks, Viruses, Malware)	55
	6.2. Use of Firewalls, Antivirus Systems, and Threat Detection Systems	57
	6.3. The Role of Security Incident Monitoring and Response	60
CHAPTER 7	PRIVACY AND DATA CONFIDENTIALITY	64
	7.1. Definition of Data Confidentiality and Privacy	64
	7.2. Policies and Regulations (GDPR, CCPA, NIST Privacy Framework)	66
	7.3. Methods of Data Anonymization and Pseudonymization	69
CHAPTER 8	IDENTIFICATION AND AUTHENTICATION IN CORPORATE SYSTEMS	73
	8.1. User Identification Methods	73
	8.2. Authentication Technologies: Passwords, Two-factor Authentication, Biometrics	74

	8.3.	Authentication Security in Corporate Networks	78
CHAPTER 9	COMMUNICATION AND DATA TRANSMISSION SECURITY		82
	9.1.	Protection of Communication Channels (VPN, SSL/TLS, Encryption)	82
	9.2.	Security Issues in Data Exchange	85
	9.3.	Detection and Prevention of Data Leaks	87
CHAPTER 10	SECURITY INCIDENT MONITORING AND RESPONSE SYSTEMS		92
	10.1	Creation of Monitoring Systems	92
	10.2	The Process of Detection, Analysis, and Response to Incidents	93
	10.3	In-depth Incident Analysis and Feedback	95
CHAPTER 11	CORPORATE NETWORK AND INFRASTRUCTURE SECURITY		102
	11.1	Network Infrastructure and Critical Services Protection	102
	11.2	Security of Protocols and Network Applications	104
	11.3	Cloud and Virtualized Environment Security	107
CHAPTER 12	CORPORATE SECURITY IMPLEMENTATION STRATEGIES		111
	12.1	Definition of Corporate Security Strategies	111
	12.2	The Importance of Developing a Security Culture in the Organization	113
	12.3	Implementation of Security Policies in the Company	116
CHAPTER 13	PLANNING AND RECOVERY AFTER SECURITY INCIDENTS		120
	13.1	Development of Incident Response Plans	120
	13.2	Recovery after Attacks and Incidents	139
	13.3	Technical and Organizational Measures to Reduce the Impact of Security Incidents	141
CHAPTER 14	AUDIT AND EVALUATION OF CORPORATE SECURITY SYSTEMS		144
	14.1	Procedure for Auditing Corporate Security	144
	14.2	Assessment of Security Systems Effectiveness	148
	14.3	Vulnerability Assessment Techniques and Security Testing	150
CHAPTER 15	PROTECTION AGAINST INTERNAL THREATS AND SOCIAL ENGINEERING		154
	15.1	Risks Associated with Internal Threats	154
	15.2	Counteraction to Social Engineering	157
	15.3	The Importance of Employee Training and Development of Security Policies	160
	LIST OF REFERENCES		163