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

TABLE OF CONTENTS