

ECONOMIC AND CYBER SECURITY

Collective monograph

UDC 658+004

E19

Published in 2023
by PC TECHNOLOGY CENTER
Shatylova dacha str., 4, Kharkiv, Ukraine, 61165

E19

Authors:

Victor Krasnobayev, Alina Yanko, Alina Hlushko, Oleg Kruk, Oleksandr Kruk, Vitalii Gakh, Svitlana Onyshchenko, Alina Yanko, Alina Hlushko, Oleksandra Maslii, Oleksandr Kivshyk, Kateryna Potapova, Mykola Nalyvaichuk, Vasyli Meliukh, Stanislav Gurynenko, Kostiantyn Koliada, Alexandre Scherbyna, Anastasiia Poltorak, Svitlana Tyshchenko, Olha Khrystenko, Volodimir Ribachuk, Vitalii Kuzoma, Viktoriia Stamat, Maksym Kolesnyk, Olena Arefieva, Dmytro Onoprienko, Yulia Kovalenko, Tetiana Ostapenko, Iryna Hrashchenko

Economic and cyber security: collective monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 196 p.

Collective monograph highlights the results of systematic scientific research devoted to the problems of economic cyber security as a component of the financial security of the state, and contains practical recommendations on measures to strengthen the security of the state, in particular strategically important enterprises, in the presence of modern threats. The problems are investigated in the following areas: the cyberspace protection system based on the method of data comparison, strategic directions and the mechanism for implementing economic cyber security in the state, strengthening the security of strategically important enterprises as a basis for supporting and restoring the national economy, in the context of the economy and cyber security using natural language processing classifiers for identification of significant information in the context of economic cyber security, theoretical and praxeological approaches to monitoring the state of financial security of the state.

The monograph is intended for researchers engaged in the development of measures to increase the financial security of the state, practitioners looking for the best scientific solutions for implementation in order to form reliable cyber protection measures in the information environment of the enterprise, contributing to the increase of its financial security, and may also be useful for state authorities.

Figures 55, Tables 23, References 206 items.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the authors. This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Trademark Notice: product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

DOI: 10.15587/978-617-7319-98-5

ISBN 978-617-7319-98-5 (on-line)




Copyright © 2023 Authors

This is an open access paper under the Creative Commons CC BY license


AUTHORS

CHAPTER 1


VICTOR KRASNOBAYEV

Doctor of Technical Sciences, Professor
Department of Electronics and Control Systems
V. N. Karazin Kharkiv National University
 ORCID ID: <https://orcid.org/0000-0001-5192-9918>

ALINA YANKO

PhD, Associate Professor
Department of Computer and Information Technologies
and Systems
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0000-0003-2876-9316>

ALINA HLUSHKO

PhD, Associate Professor
Department of Finance, Banking and Taxation
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0000-0002-4086-1513>


OLEG KRUK

Postgraduate Student
Department of Automation, Electronics and Telecommu-
nications
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0009-0004-4241-2676>

OLEKSANDR KRUK


Postgraduate Student
Department of Automation, Electronics and Telecommu-
nications
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0009-0000-7503-5249>

VITALII GAKH


Postgraduate Student
Department of Architecture of Building and Design
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0009-0003-9462-9554>

CHAPTER 2


SVITLANA ONYSHCHENKO

Doctor in Economics, Professor
Department of Finance, Banking and Taxation
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0000-0002-6173-4361>


ALINA YANKO

PhD, Associate Professor
Department of Computer and Information Technologies
and Systems
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0000-0003-2876-9316>

ALINA HLUSHKO


PhD, Associate Professor
Department of Finance, Banking and Taxation
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0000-0002-4086-1513>

OLEKSANDRA MASLII

PhD, Associate Professor
Department of Finance, Banking and Taxation
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0000-0003-2184-968X>


CHAPTER 3

OLEKSANDR KIVSHYK


Doctoral Candidate
Department of Finance, Banking and Taxation
National University "Yuri Kondratyuk Poltava Polytechnic"
 ORCID ID: <https://orcid.org/0000-0002-7154-2603>

CHAPTER 4


KATERYNA POTAPOVA

PhD, Associate Professor
Department of System Programming and Specialized
Computer Systems
National Technical University of Ukraine "Igor Sikorsky Kyiv
Polytechnic Institute"
 ORCID ID: <https://orcid.org/0000-0002-3347-6350>


MYKOLA NALYVAICHUK

PhD, Senior Lecturer
Department of System Programming and Specialized
Computer Systems
National Technical University of Ukraine "Igor Sikorsky Kyiv
Polytechnic Institute"
 ORCID ID: <https://orcid.org/0009-0009-3783-9954>


VASYL MELIUKH

Department of System Programming and Specialized
Computer Systems
National Technical University of Ukraine "Igor Sikorsky Kyiv
Polytechnic Institute"
 ORCID ID: <https://orcid.org/0009-0009-3783-9954>


STANISLAV GURYENKO

Postgraduate Student
Department of Computer-Integrated Optical and
Navigation Systems
National Technical University of Ukraine "Igor Sikorsky Kyiv
Polytechnic Institute"
 ORCID ID: <https://orcid.org/0000-0003-0180-3107>

KOSTIANTYN KOLIADA


PhD, Senior Lecturer
Department of System Programming and Specialized
Computer Systems
National Technical University of Ukraine "Igor Sikorsky Kyiv
Polytechnic Institute"
 ORCID ID: <https://orcid.org/0000-0002-3962-5791>

ALEXANDRE SCHERBYNA


PhD, Associate Professor
Department of System Programming and Specialized
Computer Systems
National Technical University of Ukraine "Igor Sikorsky Kyiv
Polytechnic Institute"
 ORCID ID: <https://orcid.org/0000-0003-0224-1441>

CHAPTER 5

ANASTASIIA POLTORAK

Doctor of Economics Sciences, Professor, Head of Department
Department of Management and Marketing
Mykolayiv National Agrarian University
 ORCID ID: <https://orcid.org/0000-0002-9752-9431>

SVITLANA TYSHCHENKO

PhD, Associate Professor, Head of Department
Department of Economic Cybernetics, Computer Sciences
and Information Technologies
Mykolayiv National Agrarian University
 ORCID ID: <https://orcid.org/0000-0001-7881-8740>

OLHA KHRYSTENKO

PhD, Associate Professor, Head of Department
Department of Business Economy
Mykolayiv National Agrarian University
 ORCID ID: <https://orcid.org/0000-0003-0431-5328>

VOLODIMIR RIBACHUK

PhD, Associate Professor
Department of Business Economy
Mykolayiv National Agrarian University
 ORCID ID: <https://orcid.org/0000-0001-9153-9674>

VITALII KUZOMA

PhD, Associate Professor
Department of Accounting and Taxation
Mykolayiv National Agrarian University
 ORCID ID: <https://orcid.org/0000-0002-6763-2120>

VIKTORIA STAMAT

PhD, Associate Professor
Department of Management and Marketing
Mykolayiv National Agrarian University
 ORCID ID: <https://orcid.org/0000-0001-5789-4023>

CHAPTER 6


MAKSYM KOLESNYK

PhD, Associate Professor
Department of Management of Foreign Economic Activity
of Enterprises
National Aviation University
 ORCID ID: <https://orcid.org/0000-0003-0814-4220>

OLENA AREFIEVA

Doctor of Economics Sciences, Professor, Head of
Department
Department of Economy of Air Transport
National Aviation University
 ORCID ID: <https://orcid.org/0000-0001-5157-9970>

DMYTRO ONOPRIENKO

Postgraduate Student
Department of Economy of Air Transport
National Aviation University
 ORCID ID: <https://orcid.org/0000-0002-9473-4464>

YULIIA KOVALENKO

PhD, Associate Professor
Department of Management of Foreign Economic Activity
of Enterprises
National Aviation University
 ORCID ID: <https://orcid.org/0000-0003-1257-3845>

TETIANA OSTAPENKO

PhD, Associate Professor
Department of Management of Foreign Economic Activity
of Enterprises
National Aviation University
 ORCID ID: <https://orcid.org/0000-0003-2032-1365>

IRYNA HRASHCHENKO

PhD, Associate Professor
Department of Management of Foreign Economic Activity
of Enterprises
National Aviation University
 ORCID ID: <https://orcid.org/0000-0002-8735-9061>

ABSTRACT

Collective monograph highlights the results of systematic scientific research devoted to the problems of economic cyber security as a component of the financial security of the state, and contains practical recommendations on measures to strengthen the security of the state, in particular strategically important enterprises, in the presence of modern threats.

Chapter 1 analyzes the position of Ukraine in the global cyber security ratings and outlines promising directions for increasing its level, one of which is the improvement of information protection systems of critical infrastructure objects. A data comparison algorithm is considered, which consists in continuous monitoring and scanning of data by constantly comparing data with information patterns of users and services, as well as threat patterns and indicators based on previous experience, not only one's own, within a local network or system, but also globally scale. An improved method of rapid data comparison is presented, which provides maximum accuracy of comparison with a minimum amount of equipment for comparing devices. Its use makes it possible to identify potential cyber threats and take preventive measures, which will increase the level of protection of critical infrastructure objects.

Chapter 2 focuses on defining strategic directions for ensuring economic cyber security of business in Ukraine. The importance of information protection in the context of the development of the digital economy has been updated, and the place of economic cyber security in the national security system has been determined. A thorough analysis of the dynamics of cyber incidents in the world in recent years was carried out and the specifics of the manifestation of cyber threats at the macro and micro levels were outlined. Special attention is paid to the intrusion detection process and a detailed study of the working principles of modern intrusion detection and prevention systems. It is expected that the use of the proposed recommendations on the cyber security policy will significantly increase the level of information security (confidentiality, integrity and availability) of the business.

Chapter 3 is dedicated to solving the problem of strengthening the security of strategically important enterprises of Ukraine by developing effective forms of implementation of the state regulatory policy in this direction. The issue of identifying strategically important enterprises and forming their security at the state level as a basis for supporting and restoring the national economy has been updated. The strategic directions of deregulation of business activity in Ukraine, including strategically important enterprises, have been determined. One of them is institutional support of state regulatory policy, improvement of regulatory policy. On the basis of the analysis of the existing institutional support of the state regulatory policy regarding strategically important enterprises, it has been proved that the basis of the formation of effective forms of implementation of the state regulatory policy of support and strengthening of the security of strategically important enterprises is the need to improve the current legislation, the formation of effective institutional and organizational support and the clustering of the national economy based on strategic important

enterprises with the possibility of creating integrated corporate structures. A model of the process of assessing the effectiveness of the implementation of the state regulatory policy on ensuring the security of strategically important enterprises is proposed, which provides regulatory bodies with a tool to influence its level with the provision of economic development and social stability in Ukraine.

Chapter 4 explores Semantic role labeling (SRL) as a key Natural Language Processing (NLP) task that plays a vital role in extracting meaningful information from text. The role of SRL and its application is considered in the context of economics and cyber security, because the accurate definition and analysis of semantic roles in text is critical due to the rapid increase in the amount and complexity of textual information. State-of-the-art NLP classifiers used in decision-making, market analysis and financial reports, media articles, and economic texts are reviewed. It is emphasized that the process of determining relevant information from a large array of data collected from disparate sources requires an optimal methodological base, which should include the use of special tools for cleaning, tokenization, marking parts of speech with labels for preparation for NLP analysis. With the help of NLP classifiers, it becomes possible to automatically identify data, which allows to get information about market trends or security threats, depending on the specific field.

Chapter 5 is dedicated to the comprehensive substantiation of the theoretical and methodological foundations and practical methods of monitoring the state of financial security of Ukraine in conditions of economic turbulence as a factor ensuring the preservation of the state's financial system. Indicators of the state of financial security of regions are proposed and it is proved that they are not strongly connected, and also interconnected with the state of financial security of the state, which allows their use as input information in the process of calculating the integral indicator of the state of financial security of the region. On the basis of the proposed methodology for assessing the state of financial security of regions, integral indicators of the state of financial security of regions of Ukraine were calculated, which are actually the result of collapsing indicators by subsystems into a system index for a certain region.

Chapter 6 discusses the essence and features of the circular economy as an innovative component of the modern economy, which functions and develops on the basis of sustainable development, the deep reasons for its emergence, formation and transformation into a factor in the formation of a new paradigm of the global economy. Being a mechanism for the implementation of the Global Goals of sustainable development, the concept of a closed cycle economy encourages highly developed countries and businesses to introduce innovations and define the development of a circular economy as a priority in their long-term strategies.

KEYWORDS

Integer economic data processing systems, modular number system, non-positional number system, economic cyber security, national economy, intrusion detection systems, unauthorized access, strategically important enterprises, state regulatory policy, institutional support, semantic role labeling, natural language processing, monitoring financial security, national security, circular economy.

CIRCLE OF READERS AND SCOPE OF APPLICATION

The monograph is intended for researchers who are engaged in the development of measures to increase the financial security of the state, primarily through the development or improvement of security systems in cyberspace, as well as practitioners who are looking for the best scientific solutions for implementation, which can contribute to the formation of reliable cyber protection measures in the information environment of the enterprise, contributing to the increase of its financial security.

The monograph is also useful for state authorities, which are forced to search for operational, most effective solutions to ensure the financial security of the state as a whole, its strategic enterprises, including critical infrastructure, in particular through the regulation of security measures in the information space, in the presence of modern external threats.

CONTENTS

List of Tables	x
List of Figures	xi
Introduction	1
1 Cyberspace protection system based on the data comparison method	3
1.1 Analysis of modern approaches to cybersecurity research	4
1.2 The level of cybersecurity of Ukraine in the conditions of growing threats.....	6
1.3 Method of arithmetic comparison of data in the MNS	12
1.4 Algebraic data comparison method in the MNS	18
1.5 Improving the method of fast comparison of two integers in the MNS	20
Conclusions	25
References.....	26
2 Economic cyber security of business in Ukraine: strategic directions and implementation mechanism	30
2.1 Risks and threats to economic cyber security of business	31
2.2 Cyber security policy strategy of business of Ukraine	37
Conclusions	54
References.....	56
3 Strengthening the security of Ukrainian strategically important enterprises as a basis for the national economy supporting and restoring	59
3.1 Assessment of the Ukrainian economic security level	60
3.2 Analysis of both business environment and state regulatory policy in the aspect of strengthening economic security under martial law.....	64
3.3 Improving the institutional support of the state regulatory policy in terms of strengthening the strategically important enterprises security in Ukraine.....	72
3.4 Modeling the process of evaluating the state regulatory policy effectiveness for ensuring strategically important enterprises strategy.....	79
Conclusions	83
References.....	84

4 Semantic role labelling and analysis in economic and cybersecurity contexts using natural language processing classifiers	88
4.1 Conventional Paradigms of empirical and rational approaches to the ambiguity of linguistic during the development of natural language processing	90
4.2 Annotating Linguistic Structure.....	94
4.3 Developing Models for Semantic Role Labeling.....	100
4.4 Methodological Foundations for Developing a Semantic Role Classifier for Cyber Threat Analysis and Economical Sphere using Artificial Neural Networks	109
Conclusions	118
References.....	119
5 Theoretical and praxeological approaches to monitoring the state of financial security of Ukraine	123
5.1 Conceptual bases for assessing the state of financial security of the state	125
5.2 Analysis of the state of financial security of Ukraine as a basis for ensuring the economic security of the state.....	130
5.3 Methodological concept of transformation of approaches to monitoring the state of financial security of Ukraine.....	149
Conclusions	155
References.....	156
6 Current issues of innovative development and evolution of the circular economy at the regional scale	160
Conclusions	179
References.....	180

LIST OF TABLES

1.1	Comparative characteristics of global indices on cybersecurity	9
1.2	Algorithm for arithmetic comparison of numbers in the MNS	14
1.3	Code word table	16
1.4	The contents of the block of nulling constant (BNC)	16
1.5	Constants for the formation of the SLBC	17
1.6	Algorithm for algebraic number comparison $S_{MNS}^{(*)}$ and $T_{MNS}^{(*)}$	19
1.7	Algorithm for arithmetic comparison of numbers in the MNS	24
3.1	Integral indicators of the Ukrainian economic security components for 2013–2020 years	62
4.1	Token label definitions of lexical parsing processes	97
5.1	Complex of indicators of the state of financial security of Ukraine	127
5.2	Input information for calculating indicators of Ukraine's debt security	131
5.3	Dynamics of Ukraine's debt security	133
5.4	The set of countries selected for comparison of levels of debt dependence of Ukraine, 2023	135
5.5	Dynamics of normalized values of indicators of Ukraine's debt security	136
5.6	Dynamics of the state of budgetary security of Ukraine	137
5.7	State dynamics of normalized indicators of budget security of Ukraine	138
5.8	Dynamics of the state of currency security of Ukraine	142
5.9	Dynamics of normalized values of indicators of the state of currency security of Ukraine	143
5.10	Dynamics of the absolute values of indicators of the banking security of Ukraine	146
5.11	Dynamics of normalized values of indicators of the state of banking security of Ukraine	147
5.12	Results of approbation of a methodical approach to monitoring the level of financial security using a polynomial correlation-regression model	153
5.13	Clustering of regions of Ukraine by ranges of values of financial security of regions of Ukraine	154
6.1	Marketing innovations of the circular economy in the activities of Ukrainian clothing brands	176

LIST OF FIGURES

1.1	Ranking of countries by the number of cyberattacks in 2021	6
1.2	Cyberattacks on critical infrastructure facilities and state information resources of Ukraine in January-February 2022	7
1.3	Global financial losses from cyberattacks in 2014–2021	8
1.4	Dynamics of Ukraine's positions in international cybersecurity rankings	9
1.5	Intervals of splitting the numerical axis $[0, D]$ for an arbitrary base m_i , MNS	15
1.6	Intervals of splitting the numerical axis $[0, D]$ for the base $m_i = 5$ MNS	15
1.7	Scheme of the procedure for comparing numbers in the MNS	17
1.8	Intervals of partitioning of the numerical axis $[0, D]$ for the base $m_i=2$ in the MNS	22
2.1	Digital Economy and Society Index, 2022	32
2.2	Economic cyber security in the national security system	33
2.3	Number of cyber incidents targeting the government sector recorded in the past two years by month	34
2.4	Number of cyber incidents targeting the government sector recorded in the past two years by country	34
2.5	The most common types of cyber attacks	36
2.6	Example of placing IDS in the network	39
2.7	Data correlation and notification process	41
2.8	Detecting the Petya virus using Azure Security Center	42
2.9	Schematic representation of IDS interaction	43
2.10	Types of existing IDS	44
2.11	Scheme of a typical IDS	46
2.12	Principle of UEBA operation	48
2.13	Detection of suspicious behavior of a network user	49
2.14	Pass-the-ticket attack detection using Microsoft ATA	49
2.15	Microsoft ATA warning to account credentials	50
2.16	Communication structure with the security center	51
2.17	Microsoft Azure Security Center Notification Panel	52
2.18	Microsoft Azure Security Center Notification Panel (analysis)	53
2.19	Alert generated by Deep Security Agent	54
3.1	Dynamics of the level of economic security of Ukraine in 2013–2020	63
3.2	Dynamics of registration of business entities, thousand units	66
3.3	Dynamics of registration, migration / relocation, bankruptcy and termination of business entities activity in Ukraine in February – December 2022	67

3.4	Dynamics of the level of financial support under the state program "Affordable loans 5–7–9 %"	71
3.5	Scheme for assessing the state regulatory policy implementation effectiveness	81
4.1	A parse tree for a sentence "The central bank raised interest rates to curb inflation"	92
4.2	Context-Free Grammar parsing example	98
4.3	Parsing type: <i>a</i> – constituency parsing (Parse tree); <i>b</i> – dependency parsing	98
4.4	The Cocke-Kasami-Younger (CKY) algorithm	100
4.5	The multilayered perceptron graph	111
4.6	The architecture of Word2Vec model	112
4.7	Vector representation of the sentences using Word2Vec model	113
4.8	Visualization of economical, cybersecurity and other non-connected words clustering	117
5.1	Classification of financial security and its role in the overall structure of the country's national security	126
5.2	Dynamics of the volumes of the state debt of Ukraine	132
5.3	Dynamics of Ukraine's GDP for 2009–2022	132
5.4	Dynamics of debt dependence of Ukraine	134
5.5	Comparative data on the structure of the total debt of Ukraine and similar countries by group, 2023	135
5.6	Dynamics of changes in the official exchange rate of Ukraine	139
5.7	Dynamics of Ukraine's international reserves	140
5.8	Loans in foreign currency in Ukraine	141
5.9	Dynamics of values of the integral index of banking security of Ukraine	148
5.10	Dynamics of the integral index of the security state of the financial system of Ukraine, %	148
6.1	Principles of 10R closed loop economy	166
6.2	Comparison of the structure of waste management in Ukraine and the EU as of 2018	172
6.3	The synergistic effect of implementing marketing innovations of the circular economy	174
6.4	Basic principles of the circular economy	176
6.5	Marketing innovations of the circular economy in the field of fashion and design	177

INTRODUCTION

The general difficult situation in the modern world requires the governments of the democratic world to take urgent measures to protect their states and citizens at all levels. Due to the aggression of the Russian Federation against Ukraine and the chain reaction that arose after the full-scale invasion of Ukraine by Russian troops on February 24, 2022, the danger in the world rose to an unprecedented level.

One of the key dangers is information security, which can cause the destruction of financial systems of national economies due to the imperfection of measures to counter unauthorized intrusions. The development of appropriate countermeasures in cyberspace is not a purely technical or technological problem, but covers much wider areas of society. In particular, counteraction mechanisms should be developed at the legislative and executive levels, which involves the involvement of many state institutions in terms of the financial security of national economies. Therefore, systemic scientific developments dedicated to both conceptual and recommendatory decisions regarding the formation of such mechanisms are relevant. It should be recognized that there are currently no single scientific and scientific-applied solutions, therefore the different views of specialists, including related fields of knowledge, on this problem are important. Among such views may be visions of some solutions to the problems of ensuring economic cyber security in the following developments: creation or improvement of cyberspace protection systems based on the comparison of available data, determination of strategic directions and implementation mechanisms for ensuring economic cyber security of business in the conditions of the development of the digital economy, solving the problem of strengthening security in a strategically important state enterprises through the development of effective forms of implementation of the state regulatory policy in this direction, methods of analysis and processing of complex textual information from various sources, comprehensive substantiation of theoretical and methodological bases and practical methods of monitoring the state of financial security of the state in conditions of economic turbulence, including those caused by external threats in the information space.

It is in this vein that the monograph presents the results of systematic research devoted to the problems of ensuring economic cyber security.

Using the example of Ukraine, the position of the state in the global cyber security ratings was analyzed and promising directions for increasing its level were outlined, one of which is the improvement of information protection systems of critical infrastructure objects. A system for protecting the information environment from cyberattacks using a modular counting system based on non-positional code structures is proposed. An improved method of quick comparison is presented, which allows the comparison procedure to be carried out in the modular counting system, both in positive and negative numerical ranges, and provides maximum accuracy of comparison with a minimum amount of equipment for comparing devices. This circumstance makes it possible to obtain

a reliable result of the data control operation, which allows identifying potential cyber threats and taking preventive measures to increase the level of protection of critical infrastructure objects.

The strategic directions of ensuring economic cyber security of business in Ukraine and the place of economic cyber security in the national security system have been determined. The modern trends of cyber threats are studied and the strategy of cyber security policy of business entities in the state is proposed. Behavioral analytics of UEBA users and objects were considered to detect violations in the field of security. On the basis of Microsoft's Advanced Threat Analytics (ATA), the process of monitoring network traffic of domain controllers was considered, with the aim of detecting cyber-attacks. Using Azure Security Center as an example, intelligent security tools and analytics enhancements are explored to detect threats faster and reduce the number of false security alerts. The use of the proposed cybersecurity policy recommendations has the potential to significantly increase the level of business information security.

The problem of strengthening the security of strategically important enterprises of Ukraine through the development of effective forms of implementation of the state regulatory policy in this direction has been studied. The issue of identifying strategically important enterprises and forming their security at the state level as a basis for supporting and restoring the national economy has been updated. With the use of the key provisions of the project of the Recovery Plan of Ukraine, strategic directions of deregulation of business activity in the state, including strategically important enterprises, have been determined.

The proposed solutions for identifying the most significant information using Natural Language Processing allow to improve decision-making processes in a digital environment that is constantly changing. This enables the analysis and understanding of security-related textual data, which in turn enables faster response to threats.

A comprehensive substantiation of the theoretical and methodological foundations and practical methods of monitoring the state of financial security of Ukraine in conditions of economic turbulence, as a factor ensuring the preservation of the state's financial system, was made. Based on this, a methodical approach to monitoring the security state of the financial stability of the regions of the state has been developed. On the basis of the proposed methodology for assessing the state of financial security of regions, integral indicators of the state of financial security of the regions of Ukraine were calculated. This makes it possible to cluster the regions of the state and to make decisions on financial security measures at the state level.

CHAPTER 1

CYBERSPACE PROTECTION SYSTEM BASED ON THE DATA
COMPARISON METHODABSTRACT

In the conditions of growing challenges in cyberspace, the information environment protection system is a preventive mechanism of protection against real and potential risks and threats to national interests. The study analyzed the position of Ukraine in the world rankings for cyber security and outlined promising directions for increasing its level, one of which is the improvement of information protection systems of critical infrastructure objects. A system of protection of the information environment against cyberattacks using of the modular number system based on non-positional code structures is proposed. Of the various options for the practice of intrusion detection and prevention systems, this chapter discusses the data comparison algorithm, which consists in continuously monitoring and scanning data by constantly comparing data with user and service information patterns, as well as threat patterns and indicators based on previous experience, not only own, within the local network or system, but also on a global scale.

The chapter presents an improved method of fast comparison, which allows to carry out the comparison procedure in the modular number system, both in positive and negative numerical ranges. Improving the method of fast comparison of two integers is carried out by increasing the accuracy of comparison, by representing numbers in an artificial form, which expands the area of effective use of computer systems for processing integer economic data in the modular number system. The use of an improved method for fast comparison of data in the modular number system for one-byte, two-byte, three-byte, four-byte and eight-byte numerical bit grids of the computer systems, respectively, by 16 %, 37 %, 50 %. It is 58 % and 72 % more efficient in terms of number comparison time than using the fastest of the existing number comparison methods in the modular number system, which is based on the principle of nulling. The proposed method provides maximum comparison accuracy with a minimum amount of equipment for comparing devices. This circumstance makes it possible to obtain a reliable result of the data control operation. Its use makes it possible to identify potential cyber threats and take preventive measures, which will increase the level of protection of critical infrastructure objects.

KEYWORDS

Arithmetic comparison, computer systems for processing integer economic data, cyberattacks, cybersecurity, cyber protection, data comparison methods, financial losses, information security, modular number system, non-positional number system, nulling constants, positional features of a non-positional code, single-line binary code, threats.

The digitalization processes rapid development gave an impetus to the development of cyberterrorism in the world. The growth of cyberattacks on critical infrastructure objects in recent years has made the information environment protecting issue as a basis for ensuring the countries national security as a whole. After all, their destructive influence extends to all the national economy spheres and is a threat to national interests. Losses from realized cyber incidents are measured not only by financial costs. The hybrid aggression of the Russian Federation against Ukraine since the beginning of 2022 has turned into a cyberwar and a full-scale military invasion. Mass cyberattacks against Ukraine state structures and businesses, which are aimed at disrupting the functioning of strategic life support facilities, require an increase in the cybersecurity level. Under the conditions of constant cyber risks and cyber threats growing the monitoring of Ukraine cybersecurity level, highlighting the main problems of national cyber protection system accretion and determination of their solving directions are important.

1.1 ANALYSIS OF MODERN APPROACHES TO CYBERSECURITY RESEARCH

The issue of cyber security is currently one of the leaders of current topics in the world, which is characterized and confirmed by active research by scientists. The issue of the formation of an effective mechanism for countering threats in the cyber sphere is clearly and in detail considered in the work of Yusif Salifu, Abdul Hafeez-Baig [1]. The authors investigated a model for effective cybersecurity management, which is based on such key components as a cybersecurity strategy, standardized processes, compliance with the requirements, senior management oversight, and resources. In the conditions of growing challenges in cyberspace, the subject of research of leading scientists are also the processes of legal support and management of cyber and information security in general, both at the national and international levels [2, 3].

The development and improvement of over-reliable computer systems (CS) is a strategically important and topical issue and is under the special control of the heads of states and governments of the advanced countries of the world. There are many approaches and tools that contribute to the stability and security of countries in cyberspace, which consist of political strategies such as the strategy of persistent engagement, recently used in the United States [4, 5] and technical methods. Among the main effective technical methods used by modern cyber

threat detection systems is the use of various data comparison methods, the main ones of which were researched by the American scientist Michael Collins [6].

The more unique and individual data protection and monitoring systems are (created exclusively for a specific object and not for mass application), the higher the level of protection against cyber-attacks has been proven by Zhang Hao Goh, Minzheng Hou, Hichang Cho [7].

Some Chinese scientists Jian Liu, Junjie Yan, Jun Jiang, Yitong He, Xuren Wang, Zhengwei Jiang and others have studied the existing positional binary number system and concluded that it has flaws, and the existing hacking methods, hacking attacks, viruses and information integrity violations are constructed using a binary positional code. Therefore, it is natural to search for opportunities to apply such arithmetic to which existing threats are not adapted [8]. In this regard, the non-positional number system (NNS) based on the Chinese residuals theorem, the so-called modular number system (MNS), draws attention. The results of research in the field of the creation of high-reliable CS of well-known authors (M. Valakh, A. Svoboda, N. Sabo, I. Y. Aksushskyi, D. I. Yudit-skyi, V. M. Glushkov, V. A. Torgashov, V. M. Amberbaev, A. A. Kolyada, A. Shimbo, P. Paulier, M. A. Thornton, R. Dreschler, D. M. Miller, and others) showed that the use of NNS as a system of calculations of CS, intended for the implementation of reliable integer arithmetic operations, significantly increases the reliability of data processing of the solution of problems of a certain class.

Indeed, as the review of the literature showed, today the field of use of the MNS is limited to a certain class of solvable problems: implementation of integer arithmetic operations of addition, subtraction and multiplication of numbers in the positive numerical range. The lack of methods of comparing integers presented in the MNS, both in the positive and negative numerical ranges, significantly narrows the area of effective use of the MNS. Therefore, when improving the method of comparing numbers, numbers were considered in the form of a string, which makes it possible to carry out an algebraic comparison of data (taking into account the sign of the number).

The purpose of the work is to research the cybersecurity of Ukraine in the conditions of military aggression, to determine the level of cyber resilience of Ukraine and directions for improving cyber protection in the terms of deepening cyberwarfare, development of data comparison methods based on non-positional code structures, which will ensure maximum accuracy for cyber intrusion detection and prevention systems.

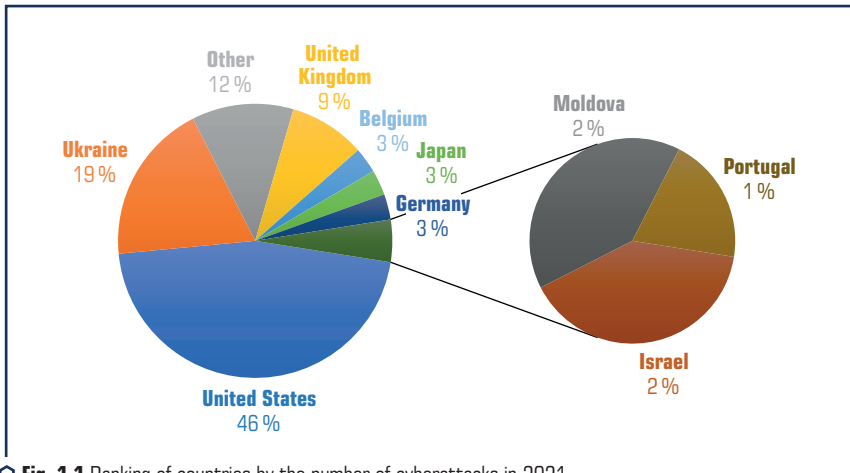
The research in the article is based on the application of data comparison principles and reliability improvement methods based on the use of non-traditional machine arithmetic. The set of properties of the MNS was used in the scientific research, namely: independence, equality, and low-bitness (low-digit capacity) of the residuals that define the non-positional code data structure of the MNS provides high reliable for the implementation in the CS of computational algorithms consisting of a set of arithmetic (modular) operations.

Using one more property of the arithmeticity of the MNS codes, which allows to find and correct errors in the process of performing arithmetic operations, which is the most important advantage of the MNS over all positional systems, including a binary code, where on the contrary, in an arithmetic device if an error occurs once, it multiply uncontrollably [9].

A distinctive feature of this article is that the proposed methods for improving the reliability of information processing in the CS, which consists in comparing data using MNS, are brought to algorithms, on the basis of which classes of patentable devices that implement such algorithms have been developed and for which Ukrainian patents have been obtained [10]. A significant part of the received patents has found practical application in the creation of specialized real-time CS for processing large arrays of integer economic data [3]. The paper gives examples of specific application of methods and algorithms for arithmetic and algebraic comparison of data in the MNS.

1.2 THE LEVEL OF CYBERSECURITY OF UKRAINE IN THE CONDITIONS OF GROWING THREATS

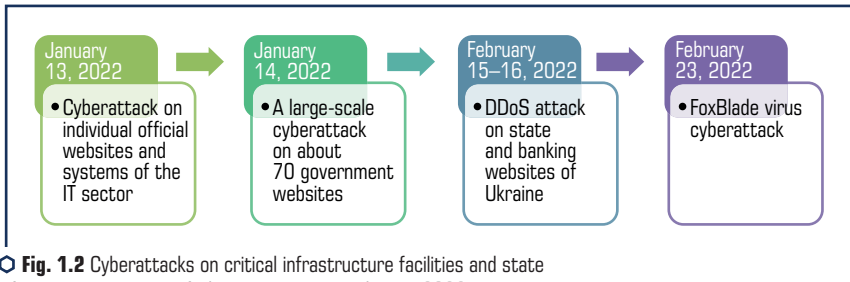
The IT technologies development, the digital environment rapid transformation along with undeniable advantages have led to the information environment risks and threats deepening [11], in cyberspace in particular. Thus, if at the beginning of 2020 the number of cyberattacks in the world was about 5 thousand per week, then at the beginning of 2021 their number increased to 200 thousand (Financial Stability Board, 2021). At the same time, 19 % of all cyberattacks in the world, recorded in 2021, were committed against Ukraine (in the first place among the countries against which cyberattacks are directed is the USA – 46 %). For comparison, the share of Belgium, Germany and Japan does not exceed 3 % (**Fig. 1.1**).



○ **Fig. 1.1** Ranking of countries by the number of cyberattacks in 2021

According to the official data of the Microsoft company [12], the largest number of cyberattacks during the II half of 2020 and the I half of 2021 were carried out from the territory of the Russian Federation – 58 % out of the entire recorded number.

According to official data, Ukraine ranks second in the world rankings in terms of the number aimed at the country's critical infrastructure, i.e. such industries as energy, finance, telecommunications, etc., and state electronic information resources, the disruption of which is a threat to national interests [13]. Since the beginning of 2022, the Russian Federation, before a full-scale invasion, has been waging a cyberwar against Ukraine – the intensity of cyberattacks is increasing: in January alone, 6.8 million suspicious information security events, 25.5 thousand potential cyber incidents and 121 cyberattacks were stopped. For comparison, in April 2021, specialists of the Security Service of Ukraine detected 1.5 million suspicious events and stopped 53 critical cyber incidents [14]. In January-February 2022, 436 cyberattacks were carried out on critical infrastructure facilities and state information resources of Ukraine, compared to 64 in the same period of 2021. The largest of them are presented in **Fig. 1.2**.



○ **Fig. 1.2** Cyberattacks on critical infrastructure facilities and state information resources of Ukraine in January-February 2022
Note: compiled by the authors according to [12, 14–16]

According to the data of the National Security Council of the United States and the National Cybersecurity Center of Great Britain, the cyberattacks were organized by the Intelligence Department of the General Staff of the Russian Federation [17, 18]. In March-May 2022, along with military aggression, cyberattacks on the energy sector, logistics infrastructure, Ukrainian online media sites, and official state resources continue.

Ransom ware, insider attacks, phishing, targeted cyberattacks and DDoS attacks are identified as the main types of cyberattacks that pose the greatest threat to the national economy information security [19]. Their destructive influence causes, first of all, significant financial losses. Thus, according to the American company McAfee, which specializes in computer security, and the Center for Strategic and International Studies (CSIS), in 2020, global economic losses as a result of cyberattacks amounted to more than 1 trillion USD, which was 1 % of global GDP. Compared to 2018, this indicator increased by more than 50 %. In 2021, losses from cyberattacks increased to 4.2–6 trillion USD (**Fig. 1.3**). It is predicted that in 2025, the volume of financial losses from cybercrime will reach 10.5 trillion USD.

It should be noted that in 2021, the highest average cost of a data breach over the past 17 years was recorded – 4.24 million USD. A similar figure for 2020 was 3.86 million USD [21].

The most common cause of data leakage was phishing attacks. In addition to direct financial losses, cyberattacks cause loss of working time, as well as the loss of the company's image [13, 22]. There are other hidden losses from cybercrime – in particular, a decrease in employee job satisfaction.

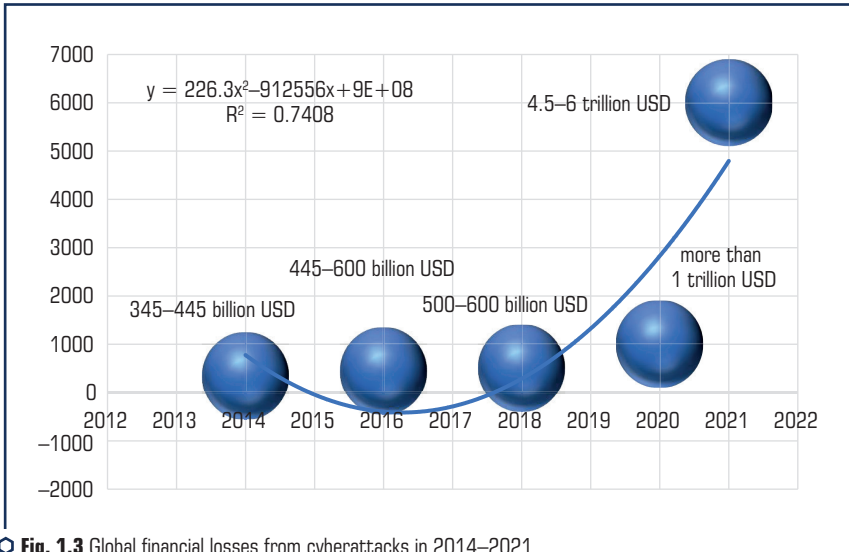


Fig. 1.3 Global financial losses from cyberattacks in 2014–2021

Note: compiled by the authors according to [20]

Taking into account the growth of negative financial consequences from the cyber threat's implementation, the need to increase the cybersecurity level under the circumstances of a cyberwar with the Russian Federation is unconditional.

To date, a number of global indices have been developed which allow determining the country capabilities in the field of cyber protection, assessing its cyber power, specifically, the regulatory measures and means ability to achieve strategic cybersecurity goals. Ukraine's high potential in this direction should be noted. This is confirmed by the positions in the world rankings, the comparative characteristics of which are presented in **Table 1.1**.

According to the National Cybersecurity Index (NCSI), which measures the countries readiness to prevent cyber threats and manage cyber incidents, Ukraine rose to 24th place among 160 countries at the end of 2021 and improved its position by 4 points compared to 2019. Ukraine is approaching Switzerland (23rd place) and Great Britain (22nd place) in terms of cyber protection capabilities of the national information space. At the same time, according to the Global Cybersecurity Index (GCI), Ukraine ranks 78th. According to the National Cyber Prowess Index (NCPI), which measures the effectiveness of government strategy, crime response and countermeasures, defense capabilities, resource allocation, private sector participation, workforce efficiency and

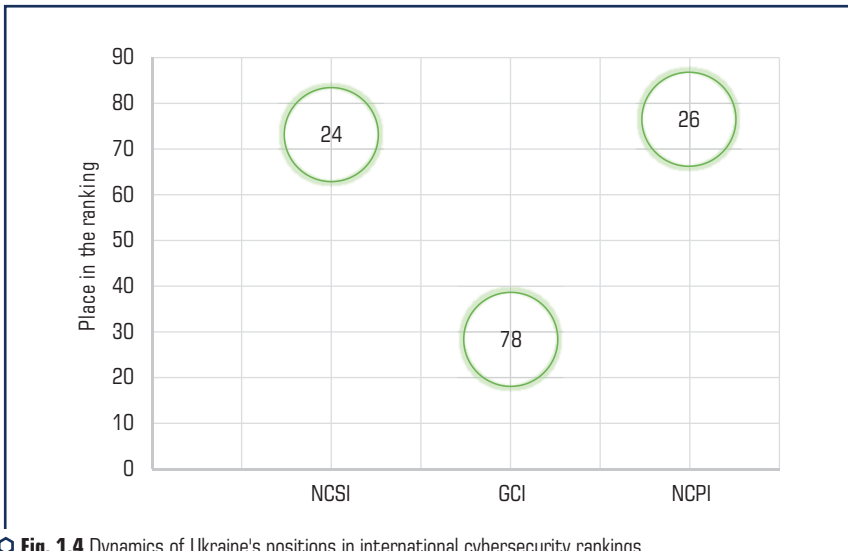
cybersecurity innovation, in 2020, Ukraine ranked only 26th out of 30 countries in the world and 10th among European countries. At the same time, it should be noted that the countries that had the most developed cybersecurity forces were included in the rating, which confirms the existence of potential opportunities for building up cyber capabilities and increasing the level of information security in Ukraine.

Graphical interpretation of Ukraine's positions in the world cybersecurity rankings and their dynamics are presented in **Fig. 1.4**.

◆ **Table 1.1** Comparative characteristics of global indices on cybersecurity

	National Cybersecurity Index (NCSI)	Global Cybersecurity Index (GCI)	National Cyberpower Index (NCPI)
Published last year	2021	2021	2020
Developer	Estonian Academy of e-Government	International Telecommunications Union	Belfer center
Countries Assessed	160	194	30
Indicators	12 General cybersecurity indicators	20 indicators	27 Capability 32 Intent
Ukraine's place in the ranking	24	78	26

Note: compiled by the authors according to [23–25]



○ **Fig. 1.4** Dynamics of Ukraine's positions in international cybersecurity rankings

Note: compiled by the authors according to [23–25]

The potential of Ukraine in the field of cybersecurity is noted not only by world ratings, but also by international organizations. Among other things, at the beginning of April 2022, Ukraine was admitted to the NATO Cooperative Cyber Defence Centre of Excellence as a contributing member.

The positive dynamics connected, *inter alia*, with the improvement of domestic legislation in the field of information and cybersecurity is noted. At present, the legal framework for regulating and ensuring security in the information space, including cyberspace, includes: the Constitution of Ukraine, the Law of Ukraine "On National Security of Ukraine", the Law of Ukraine "On the Concept of the National Informatization Program", the Law of Ukraine "On Basic Principles of the Development of the Information Society Development in Ukraine for 2007–2015", National Security Strategy, Information Security Strategy, Cybersecurity Strategy of Ukraine, Concept for the Development of the Digital Economy and Society of Ukraine for 2018–2020, Concept for the Development of Digital Competences, International Standards of the ISO/IEC 27000 series, regulatory papers in the field of information technical defense (RP ITD) and national standards of Ukraine on creating and functioning of CSID, other regulatory law acts which control interactions on the field of information defense.

The strengthening of cooperation with international organizations in the field of cybersecurity is also noted. In September 2021, the State Service for Special Communications and Information Protection of Ukraine made an agreement with the US Agency for Cybersecurity and Infrastructure Security, which provides: coordination of actions to protect critical information infrastructure objects and improvement of the response system to cyber incidents; exchange of experience within the framework of the risk management system, which will ensure Ukraine's national resilience to cyber threats; use of the US experience in organizing the government bodies interaction and business in the field of cybersecurity; implementation of international technical assistance projects related to the construction of a network of branch and regional Security Operation Center and Computer Security Incident Response Team (CSIRT) which are implied by the Strategy of Cybersecurity of Ukraine.

The accession of Ukraine to the Joint Center of Advanced Technologies for NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which took place in April 2022, provides an opportunity to exchange experience in detecting and countering modern cyber threats, practicing the skills of joint response to cyberattacks and conducting defense and deterrence operations in cyberspace.

The development of international cooperation in the direction of strengthening Ukraine's cyber resilience is a priority task in order to prevent global information threats, ensure a high-level quality of cybercrime investigations, arrest and prosecute malicious agents, and overcome cybersecurity problems.

At the same time, there are directions in the field of cybersecurity that have a negative impact on Ukraine's position in the specified ratings and require improvement. In particular, the low level of contribution to global cybersecurity to date, the insufficient level of digital services protection, the insufficiently developed direction of military cyber operations.

It should be noted that since the beginning of 2022, vigorous activities have been conducted in all the noted problematic aspects: Ukraine has become an active participant in international cooperation in the field of cybersecurity; there is a process of forming a cyber-army [26, 27], which is responsible for information security, protection of critical infrastructure and intelligence.

Considering Ukraine's achievements in cyberspace, it is legitimate to define it as an equal participant in the international arena in the field of cybersecurity. Prospective tasks should be the further improvement of information protection systems of critical infrastructure objects based on best global practices, as well as the coordination of actions with international organizations to counter threats related to the development of the digital economy and information society.

The construction of an effective cybersecurity system in the aspect of comprehensive counteraction to cyber threats will contribute to the formation of a preventive mechanism for countering threats and their containment, anticipatory response to dynamic changes occurring in cyberspace, which is necessary in the conditions of cyberwar. Methods and algorithms of security systems against unauthorized intruders are, as a rule, developed for a specific object of protection. But regardless of the protection object, whether it is a large commercial network, a state-level server, or a simple user's mobile device, there is one common goal, which is to protect data as the main element of information security.

In order to protect any system, it is necessary first to detect an intrusion (attack) regardless of the type, whether it will be viruses (classic file viruses or ransomware viruses, so-called Ransomware encryptors), phishing, DDoS attacks, botnets, backdoors, or other hacking attempts it is the task of Intrusion Detection System (IDS). The next step is to decide how to eliminate this cyberattack and, based on this experience, create a reliable algorithm for protection against threats of this type, this is the task of Intrusion Prevention System (IPS). There are various modes of systems for detecting and preventing intruders, but, as a rule, the algorithm is the same, when detecting and eliminating attacks, the task of security systems is also to create templates of potential threats. In the further process of continuous data monitoring and scanning, a constant comparison of data with user templates and service information, as well as with threats templates and indicators based on previous experience, not only within the local network or system, but also on a global scale [6].

At the moment there are various programs (Azure Security Center, Microsoft Advanced Threat Analytics) with a templates database of all threats that had been identified before that in the world. Also, there are many sites with which you can get information about new indicators and templates, as well as make your own contribution to the cyber protection IT community by sharing your types of attacks, if they are not available on this platform [28].

It is very important that cyberattack protection systems compare all data on a wide scale and make correlations not only by the traffic pattern, but also by the user profile, since otherwise the chances of false positives increase. It is possible to use different security centers, software and hardware protection, but all of them make decisions as a result of monitoring based on certain data comparison methods. Since all data is presented in the form of a binary code, the task is reduced to comparing numbers [29].

In previous studies, the advantage of using computer systems for processing integer economic data (CSPIED) based on the system of final classes was proven modular number system (MNS). It is known that using a non-positional number system in the MNS enables the organization of

integer data rapid processing procedure, i.e. the possibility of creating methods and tools that provide high user productivity in solving a certain class of problems (implementation of arithmetic operations of addition, subtraction, multiplication). This is achieved due to the use of such properties of the MNS as independence and small-scale residuals $\{s_i\}$, the set of which is a number $S_{MNS} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)$ according to n bases (modules m_n) of this MNS, by using tabular machine arithmetic. The need to perform non-positional operations of comparing two numbers $S_{MNS} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n)$ when solving GSPIED problems and algorithms of various purposes reduces the overall efficiency of using MNS. This is due to the significant implementation time (compared to the time of performing the above-mentioned arithmetic operations) of the comparing two numbers in the MNS operation. Therefore, the research and development of mathematical models, methods and algorithms for comparing numbers in the MNS is an important and urgent task [30].

At present, it is possible to distinguish three groups of methods of comparing numbers in the MNS. The first group includes methods of direct comparison based on the transformation of numbers S_{MNS} and T_{MNS} from the MNS code to the positional number system (PNS) $S_{PNS} = \overline{s_{m-1}, s_{m-2}, \dots, s_0}$ and $T_{PNS} = \overline{t_{m-1}, t_{m-2}, \dots, t_0}$ (p – digits of numbers S_{MNS} and T_{MNS}) and their further comparison based on the use of binary positional adders. The second group of methods includes methods based on the principle of nulling. The procedure of the nulling process consists of moving from the initial number $S_{MNS} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)$ presented in the MNS to the species $S_{MNS}^{(N)} = (0, 0, \dots, 0, \chi_n^{(S)})$. After that, by value $\chi_n^{(S)}$ the interval $[gm_i, (g+1)m_i)$ hitting numbers S_{MNS} is determined. Nulling of the number is carried out similarly $T_{MNS} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n)$, from where let's get the values $\chi_n^{(T)}$. Positional comparison of the obtained values $\chi_n^{(S)}$ and $\chi_n^{(T)}$ determines the result of comparing numbers S_{MNS} and T_{MNS} . The third group of methods includes methods based on the determination (selection) or formation of special features, so-called positional features of a non-positional code (PFNC). PFNC data (for example, rank r numbers S_{MNS}) carry additional information about the magnitude of the numbers that are compared [31].

The common disadvantages of all currently existing groups of methods comparisons are the time and hardware complexity of organizing an effective comparison, as well as the possibility of obtaining an unreliable result of comparing two numbers operation due to calculated errors. The abovementioned material is the basis for using a new comparison method.

1.3 METHOD OF ARITHMETIC COMPARISON OF DATA IN THE MNS

Let's consider the numbers arithmetic comparison method of $S_{MNS} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n)$, based on the use of PFNC of these numbers, by forming a single-line binary code (SLBC). Let the MNS be given by the set $\{m_i\}$, $i = \overline{1, n}$, pairs of prime numbers. The greatest common divisor (GCD) of any pair is based on m_i and m_g ($i, g = \overline{1, n}$; $i \neq g$) is equal to unity, i.e., $\text{GCD}(m_i, m_g) = 1$. For the sake of common sense, let the MNS be ordered ($m_i < m_{i+1}$).

The essence of the proposed method is that the initial numbers S_{MNS} and T_{MNS} by means of nulling constants (NC) of the form $NC_{m_i}^{(S)} = (s'_1, s'_2, \dots, s'_{j-1}, s_j, s'_{j+1}, \dots, s'_n)$ and $NC_{m_i}^{(T)} = (t'_1, t'_2, \dots, t'_{j-1}, t_j, t'_{j+1}, \dots, t'_n)$ are reduced to numbers $S_{v_i} = S_{MNS} - NC_{m_i}^{(S)} = (s_1, s_2, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_n) - (s'_1, s'_2, \dots, s'_{j-1}, s_j, s'_{j+1}, \dots, s'_n) = (s_1^{(1)}, s_2^{(1)}, \dots, s_{j-1}^{(1)}, 0, s_{j+1}^{(1)}, \dots, s_n^{(1)})$, $T_{m_i} = T_{MNS} - NC_{m_i}^{(T)} = (t_1, t_2, \dots, t_{j-1}, t_j, t_{j+1}, \dots, t_n) - (t'_1, t'_2, \dots, t'_{j-1}, t_j, t'_{j+1}, \dots, t'_n) = (t_1^{(1)}, t_2^{(1)}, \dots, t_{j-1}^{(1)}, 0, t_{j+1}^{(1)}, \dots, t_n^{(1)})$, a multiple of a certain chosen one p_i MNS module. Further, by means of the aggregate $0, m_i, 2 \cdot m_i, \dots, (N-2) \cdot m_i, (N-1) \cdot m_i$ of N constants multiples of the base m_i , subtraction operations are carried out in parallel in time $S_{m_i} - K_S \cdot m_i = Z_{K_S}^{(S)}$ and $T_{m_i} - K_T \cdot m_i = Z_{K_T}^{(T)}$, ($K_S(K_T) = \overline{0, N-1}$) that:

$$\begin{cases} S_{m_i} - 0 \cdot m_i = Z_0^{(S)}, & T_{m_i} - 0 \cdot m_i = Z_0^{(T)}, \\ S_{m_i} - 1 \cdot m_i = Z_1^{(S)}, & T_{m_i} - 1 \cdot m_i = Z_1^{(T)}, \\ S_{m_i} - 2 \cdot m_i = Z_2^{(S)}, & T_{m_i} - 2 \cdot m_i = Z_2^{(T)}, \\ \dots & \dots \\ S_{m_i} - (N-1) \cdot m_i = Z_{N-1}^{(S)}, & T_{m_i} - (N-1) \cdot m_i = Z_{N-1}^{(T)}, \end{cases} \quad (1.1)$$

where

$$N_{m_i} = \prod_{k=1; k \neq i}^n m_k,$$

N_{m_i} – the number of binary digits in SLBC records $K_{N_{m_i}}^{(n_S)}$ and $K_{N_{m_i}}^{(n_T)}$ or the number of adders performing type operations $S_{m_i} - K_S \cdot m_i = Z_{K_S}^{(S)}$ or $T_{m_i} - K_T \cdot m_i = Z_{K_T}^{(T)}$.

Thus, an SLBC of the binary sequence type is formed $K_{N_{m_i}}^{(n_S)} = \{Z_{N_{m_i}-1}^{(S)} Z_{N_{m_i}-2}^{(S)} \dots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)}\}$ for the number S_{MNS} , with only one value $Z_{K_S}^{(S)} = 0$. In the case that $S_{m_i} - n_S \cdot m_i = 0$. Other values $Z_{K_S}^{(S)} = 1$, if $S_{m_i} - q \cdot m_i \neq 0$, $q = \overline{0, N-1}$, $q \neq n_S$. In this case, the SLBC is issued $K_{N_{m_i}}^{(n_S)}$ and $K_{N_{m_i}}^{(n_T)}$ is a sequence consisting of N_{m_i} binary levels. In this sequence, only one binary digit is zero, and the rest are ones. Locations of zero discharges of the SLBC $K_{N_{m_i}}^{(n_S)}$ and $K_{N_{m_i}}^{(n_T)}$ determine PFNC n_S and n_T respectively, the numbers S_{MNS} and T_{MNS} . In a similar way, the SLBC of the form is formed $K_{N_{m_i}}^{(n_T)} = \{Z_{N_{m_i}-1}^{(T)} Z_{N_{m_i}-2}^{(T)} \dots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)}\}$ for the number T_{MNS} . At the same time, the meaning $Z_{K_T}^{(T)} = 0$ (if $T_{m_i} - n_T \cdot m_i = 0$), and the other values $Z_{K_T}^{(T)} = 1$, if $T_{m_i} - q \cdot m_i \neq 0$ ($q = \overline{0, N-1}$, $q \neq n_T$) [9].

The method of arithmetic comparison of two numbers in the MNS consists in performing the following steps of the algorithm:

1. Representation of compared numbers in the MNS:

$$S_{MNS} = (s_1, s_2, \dots, s_{j-1}, s_j, s_{j+1}, \dots, s_n)$$

and

$$T_{MNS} = (t_1, t_2, \dots, t_{j-1}, t_j, t_{j+1}, \dots, t_n).$$

2. Formation by values s_n and t_n of nulling constants of the species:

$$NC_{m_i}^{(S)} = (s'_1, s'_2, \dots, s'_{i-1}, s_i, s'_{i+1}, \dots, s'_n)$$

and

$$NC_{m_i}^{(T)} = (t'_1, t'_2, \dots, t'_{i-1}, t_i, t'_{i+1}, \dots, t'_n).$$

3. Determining the values of the difference of numbers S_{m_i} and T_{m_i} :

$$\begin{aligned} S_{m_i} &= S_{MNS} - NC_{m_i}^{(S)} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n) - (s'_1, s'_2, \dots, s'_{i-1}, s_i, s'_{i+1}, \dots, s'_n) = \\ &= (s_1^{(1)}, s_2^{(1)}, \dots, s_{i-1}^{(1)}, 0, s_{i+1}^{(1)}, \dots, s_n^{(1)}) \end{aligned}$$

and

$$\begin{aligned} T_{m_i} &= T_{MNS} - NC_{m_i}^{(T)} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n) - (t'_1, t'_2, \dots, t'_{i-1}, t_i, t'_{i+1}, \dots, t'_n) = \\ &= (t_1^{(1)}, t_2^{(1)}, \dots, t_{i-1}^{(1)}, 0, t_{i+1}^{(1)}, \dots, t_n^{(1)}). \end{aligned}$$

4. Definition of the SLBC components $z_i^{(S)}$ and $z_g^{(T)}$:

$$K_{N_{m_i}}^{(n_s)} = \{Z_{N_{m_i}-1}^{(S)} Z_{N_{m_i}-2}^{(S)} \dots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)}\}$$

and

$$K_{N_{m_i}}^{(n_T)} = \{Z_{N_{m_i}-1}^{(T)} Z_{N_{m_i}-2}^{(T)} \dots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)}\}.$$

By means of adders, using a set of constants $(0, m_i, \dots, (N-1) \cdot m_i)$ by formulas $S_{m_i} - K_S \cdot m_i = Z_{K_S}^{(S)}$ and $T_{m_i} - K_T \cdot m_i = Z_{K_T}^{(T)}$ components are defined $z_i^{(S)}$ and $z_g^{(T)}$.

5. Formation of quantitative values of PFNC n_S and n_T . By type of the SLBC $K_{N_{m_i}}^{(n_s)} = \{Z_{N_{m_i}-1}^{(S)} Z_{N_{m_i}-2}^{(S)} \dots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)}\}$ and $K_{N_{m_i}}^{(n_T)} = \{Z_{N_{m_i}-1}^{(T)} Z_{N_{m_i}-2}^{(T)} \dots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)}\}$ the values of the binary digits of the SLBC are determined for which $Z_{n_s}^{(S)} = 0$ and $Z_{n_T}^{(T)} = 0$.

6. Implementation of the comparison operation result algorithm S_{MNS} and T_{MNS} :

$$S_{MNS} = T_{MNS}, \text{ if } (n_S = n_T); S_{MNS} > T_{MNS}, \text{ if } (n_S > n_T); S_{MNS} < T_{MNS}, \text{ if } (n_S < n_T).$$

● **Table 1.2** Algorithm for arithmetic comparison of numbers in the MNS

No.	Number comparison result	Condition for performing comparison operations
1	$S_{MNS} = T_{MNS}$	$n_S = n_T$
2	$S_{MNS} > T_{MNS}$	$n_S > n_T$
3	$S_{MNS} < T_{MNS}$	$n_S < n_T$

To illustrate the essence of the comparison method, let's consider the geometric interpretation of the proposed method for comparing two numbers. **Fig. 1.5** presents a numerical segment $[0, D]$, corresponding to the range of representation of the compared numbers $S_{MNS} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n)$, where $D = \prod_{i=1}^n m_i$. This segment is divided into intervals $[gm_i, (g+1)m_i]$, of length m_i units each. The operation of converting the initial numbers S_{MNS} and T_{MNS} via nulling constants $NC_{m_i}^{(S)} = (s'_1, s'_2, \dots, s'_{i-1}, s_i, s'_{i+1}, \dots, s'_n)$ and $NC_{m_i}^{(T)} = (t'_1, t'_2, \dots, t'_{i-1}, t_i, t'_{i+1}, \dots, t'_n)$ to the species:

$$\begin{aligned} S_{m_i} &= S_{MNS} - NC_{m_i}^{(S)} = (s_1, s_2, \dots, s_{k-1}, s_k, s_{k+1}, \dots, s_n) - (s'_1, s'_2, \dots, s'_{i-1}, s_i, s'_{i+1}, \dots, s'_n) = \\ &= (s_1^{(1)}, s_2^{(1)}, \dots, s_{i-1}^{(1)}, 0, s_{i+1}^{(1)}, \dots, s_n^{(1)}) \end{aligned}$$

and

$$\begin{aligned} T_{m_i} &= T_{MNS} - NC_{m_i}^{(T)} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n) - (t'_1, t'_2, \dots, t'_{i-1}, t_i, t'_{i+1}, \dots, t'_n) = \\ &= (t_1^{(1)}, t_2^{(1)}, \dots, t_{i-1}^{(1)}, 0, t_{i+1}^{(1)}, \dots, t_n^{(1)}) \end{aligned}$$

is equivalent to shifting comparable numbers to the left edge of the corresponding intervals $[g_i m_i, (g_i + 1)m_i]$ and $[g_2 m_i, (g_2 + 1)m_i]$ their initial location, which corresponds to reducing them to numbers S_{m_i} and T_{m_i} , multiple modulo m_i MNS. Then the numbers are determined $g_1 = n_s$ and $g_2 = n_t$ these intervals (see expression (1)), which is the PFNC of numbers in the MNS.

Consider an example of a specific implementation of the operation of arithmetic comparison of numbers in the MNS with bases $m_1 = 2$, $m_2 = 3$ and $m_3 = 5$, where in $D = \prod_{i=1}^n m_i = 2 \cdot 3 \cdot 5 = 30$; $N_{m_i} = \prod_{k=1, k \neq i}^n m_k = N_{m_3} = N_5 = \prod_{k=1, k \neq 3}^2 m_k = m_1 \cdot m_2 = 2 \cdot 3 = 6$ (**Fig. 1.6**). **Table 1.3** shows the code words for this MNS. **Table 1.4** shows the NC and **Table 1.5** shows the sets of constants in the MNS with bases $m_1 = 2$, $m_2 = 3$ and $m_3 = 5$.

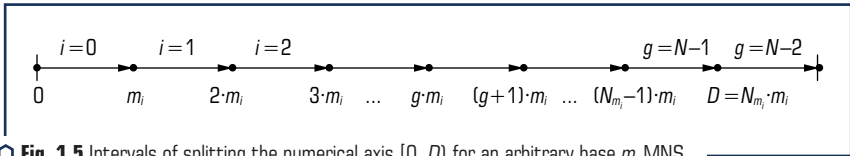


Fig. 1.5 Intervals of splitting the numerical axis $[0, D]$ for an arbitrary base m_i MNS

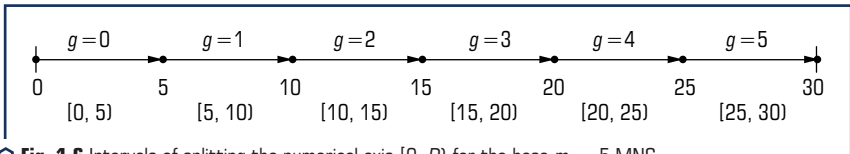


Fig. 1.6 Intervals of splitting the numerical axis $[0, D]$ for the base $m_i = 5$ MNS

The application of the considered method enables to carry out an exact comparison of two numbers only if these numbers are found in different numerical intervals $[g_1m_i, (g_1 + 1)m_i)$ and $[g_2m_i, (g_2 + 1)m_i)$. When the values are equal to numbers $g_1 = g_2 = g$, the accuracy of the comparison depends on the size of the interval $[gm_i, (g + 1)m_i)$, i.e. from the value of the value of the MNS module.

● **Table 1.3** Code word table

$S(T)$ in PNS	$S_{MNS}(T_{MNS})$ in the MNS			$S(T)$ in PNS	$S_{MNS}(T_{MNS})$ in the MNS		
	$m_1=2$	$m_2=3$	$m_3=5$		$m_1=2$	$m_2=3$	$m_3=5$
0	0	00	000	15	1	00	000
1	1	01	001	16	0	01	001
2	0	10	010	17	1	10	010
3	1	00	011	18	0	00	011
4	0	01	100	19	1	01	100
5	1	10	000	20	0	10	000
6	0	00	001	21	1	00	001
7	1	01	010	22	0	01	010
8	0	10	011	23	1	10	011
9	1	00	100	24	0	00	100
10	0	01	000	25	1	01	000
11	1	10	001	26	0	10	001
12	0	00	010	27	1	00	010
13	1	01	011	28	0	01	011
14	0	10	100	29	1	10	100

● **Table 1.4** The contents of the block of nulling constant (BNC)

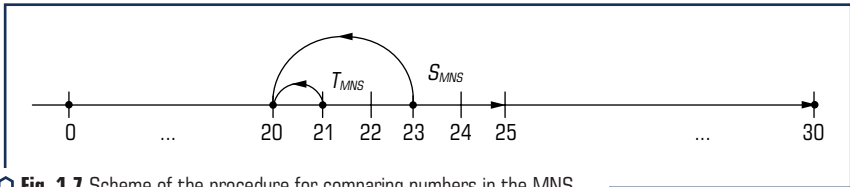
$s_3(t_3)$	Constants		
	$m_1=2$	$m_2=3$	$m_3=5$
000	0	00	000
001	1	01	001
010	0	10	010
011	1	00	011
100	0	01	100

● **Table 1.5** Constants for the formation of the SLBC

$g \cdot m_2 (g = 0, 5)$	Constants in the MNS		
	$m_1=2$	$m_2=3$	$m_3=5$
0	0	00	000
5	1	10	000
10	0	01	000
15	1	00	000
20	0	10	000
25	1	01	000

Let's give an example of the implementation of the operation of comparing two numbers for the case $g_1 = g_2 = g$.

Example 1. Let the compared operands $S=23 (S_{MNS}=(1, 10, 011))$ and $T=21 (T_{MNS}=(1, 00, 001))$ will be presented in the form in the MNS (**Fig. 1.7**).



○ **Fig. 1.7** Scheme of the procedure for comparing numbers in the MNS

By residue values s_n and t_n , where $s_n = 011$, $t_n = 001$ choose from BNC (**Table 1.4**) nulling constants, which have the form $NC_{m_n}^{(S)} = (1, 00, 011)$ and $NC_{m_n}^{(T)} = (1, 01, 001)$. Next, define the numbers $S_{m_n} = S_{MNS} - NC_{m_n}^{(S)} = (1, 10, 011) - (1, 00, 011) = (0, 10, 000)$ and $T_{m_n} = T_{MNS} - NC_{m_n}^{(T)} = (1, 00, 001) - (1, 01, 001) = (0, 10, 000)$, which corresponds to operand shift S_{23} and T_{21} to the left edge of the interval $[20, 25]$ (**Fig. 1.7**) their hits. Further, for the input operands, by means of the implementation of expression (1.1), form the SLBC of the form $K_{N_{m_n}}^{(n_S)} = K_6^{(4)} = \{101111\}$, and $K_{N_{m_n}}^{(n_T)} = K_6^{(4)} = \{101111\}$, where $N_5 = \prod_{n=1}^{i-1} m_n = 6$ and $n_S = n_T = 4$. Because $n_S = n_T = 4$, then it is considered that $S_{MNS} = T_{MNS}$. Actually $S = 23 > T = 21$. This disadvantage of the comparison method is due to the following. In the case of comparing numbers in the MNS, the accuracy W_{m_i} comparing two numbers $S_{MNS} = (s_1, s_2, \dots, s_{j-1}, s_j, s_{j+1}, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_{j-1}, t_j, t_{j+1}, \dots, t_n)$, depends on the location of the intervals $[g, m_i, (g+1)m_i)$ and $[g_2 m_i, (g_2+1)m_i)$ finding these numbers on the numerical axis $0 \div D$ (**Fig. 1.5**), i.e. from intervals g_1 and g_2 . For values equal to given numbers $g_1 = g_2 = g$, accuracy W_{m_i} comparison depends on the size of the interval $[g m_i, (g+1)m_i)$, i.e. from the value of the quantity m_i MNS module. For this case $g_1 = g_2 = g$ have the following

equality $S_{m_i} = T_{m_i} = g \cdot m_i$. This testifies that $S_{MNS} = T_{MNS}$. However, this is not always true. In accordance with the considered method of comparison, all numbers that fall into the numerical interval $[gm_i, (g+1)m_i]$ will be equal to each other. This circumstance causes the unsuitability of this method of comparing data in the MNS for all variants of the values of the compared numbers.

1.4 ALGEBRAIC DATA COMPARISON METHOD IN THE MNS

Based on the method of arithmetic comparison proposed in subsection 4, let's move on to a possible implementation of the operation of algebraic comparison of two numbers in the MNS. Perhaps there are two fundamentally possible options for organizing the procedure for algebraic comparison: the introduction of a sign in explicit and implicit (using the artificial form (AF) representation of the compared numbers) forms. Let's consider the first option. In this case, the compared operands $S_{MNS} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n)$ additionally have two iconic discharges $\Delta_{+S} (\Delta_{+T})$ and $\Delta_{-S} (\Delta_{-T})$, where:

$$\Delta_{+S} (\Delta_{+T}) = \begin{cases} 1, & \text{if } S_{MNS} (T_{MNS}) > 0, \\ 0, & \text{if } S_{MNS} (T_{MNS}) < 0; \end{cases} \quad \Delta_{-S} (\Delta_{-T}) = \begin{cases} 0, & \text{if } S_{MNS} (T_{MNS}) > 0, \\ 1, & \text{if } S_{MNS} (T_{MNS}) < 0. \end{cases} \quad (1.2)$$

Thus, the compared operands are represented as:

$$\begin{aligned} S_{MNS}^{(*)} &= \{\Delta_{+S}, \Delta_{-S}; S_{MNS}\} = \{\Delta_{+S}, \Delta_{-S}; (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)\}; \\ T_{MNS}^{(*)} &= \{\Delta_{+T}, \Delta_{-T}; T_{MNS}\} = \{\Delta_{+T}, \Delta_{-T}; (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n)\}, \end{aligned} \quad (1.3)$$

where $\Delta_{+S} (\Delta_{+T})$ – positive and $\Delta_{-S} (\Delta_{-T})$ – negative features of algebraic numbers, respectively $S_{MNS}^{(*)}$ and $T_{MNS}^{(*)}$ in the MNS.

Example 1. Compare two numbers $S^{(*)} = 21$ and $T^{(*)} = -24$. Taking into account expressions (1.2) and (1.3), represent the compared operands in the form $S_{21}^{(*)} = \{(1, 0; (1, 00, 001))\}$ and $T_{-24}^{(*)} = \{(0, 1; (0, 00, 100))\}$ in the MNS. By the value of the residuals $s_n = s_3 = 001$ and $t_n = t_3 = 100$ choose from BNC (**Table 1.4**) nulling constants which has the form $NC_{m_n}^{(S)} = (1, 01, 001)$ and $NC_{m_n}^{(T)} = (0, 01, 100)$. Next, define the numbers, $S_{m_n} = S_{MNS} - NC_{m_n}^{(S)} = (1, 10, 011) - (1, 00, 011) = (0, 10, 000)$ and $T_{m_n} = T_{MNS} - NC_{m_n}^{(T)} = (1, 00, 001) - (1, 01, 001) = (0, 10, 000)$, which corresponds to operand shift $S_{21} = |S_{21}^{(*)}|$ and $T_{24} = |T_{-24}^{(*)}|$ to the left edge of the interval $[20, 25]$.

Further, through the implementation of expression (1.1), the SLBC is formed for the input operands $S_{21} = |S_{21}^{(*)}|$ and $T_{24} = |T_{-24}^{(*)}|$ as $K_{N_n}^{(n_s)} = K_6^{(4)} = \{101111\}$, $K_{N_n}^{(n_t)} = K_6^{(4)} = \{101111\}$, where $N_5 = \prod_{n=1}^{i-1} m_n = 6$ and $n_s = n_t = 4$. At the same time, through $(n = \lceil \log_2(t_n - 1) \rceil + 1)$ -bit comparison circuit, the result of comparison of residuals is determined in parallel in time $s_n = 001 < t_n = 100$. Because $n_s = n_t = 4$, $\Delta_{+S} = 1$ and $\Delta_{-T} = 1$, then in accordance with the algorithm of algebraic

comparison (**Table 1.6**) determine that $S_{21}^{(s)} > T_{-24}^{(t)}$. Check: $21 > -24$. The disadvantage of the previous comparison method, which was the low accuracy of the comparison, was eliminated.

● **Table 1.6** Algorithm for algebraic number comparison $S_{MNS}^{(s)}$ and $T_{MNS}^{(t)}$

No.	Number comparison result	Condition for performing comparison operations
1	$S_{MNS}^{(s)} = T_{MNS}^{(t)}$	$\{(n_s = n_t) \wedge (\Delta_{+s} \wedge \Delta_{+t})\} \vee \{(n_s = n_t) \wedge (\Delta_{-s} \wedge \Delta_{-t})\}$
2	$S_{MNS}^{(s)} > T_{MNS}^{(t)}$	$\{(n_s = n_t) \wedge (\Delta_{+s} \wedge \Delta_{-t})\} \vee \{(n_s > n_t) \wedge (\Delta_{+s} \wedge \Delta_{+t})\} \vee \{(n_s > n_t) \wedge (\Delta_{+s} \wedge \Delta_{-t})\} \vee \{(n_s < n_t)\} \wedge \{(\Delta_{+s} \wedge \Delta_{-t})\} \vee \{(n_s < n_t)\} \wedge \{(\Omega_{-s} \wedge \Omega_{-t})\}$
3	$S_{MNS}^{(s)} < T_{MNS}^{(t)}$	$\{(n_s = n_t) \wedge (\Delta_{-s} \wedge \Delta_{+t})\} \vee \{(n_s > n_t) \vee (\Delta_{-s} \wedge \Delta_{+t})\} \vee \{(n_s > n_t) \wedge (\Delta_{-s} \wedge \Delta_{-t})\} \vee \{(n_s < n_t)\} \wedge \{(\Delta_{+s} \wedge \Delta_{+t})\} \vee \{(n_s < n_t)\} \wedge \{(\Delta_{-s} \wedge \Delta_{+t})\}$

Consider the second version of the method of algebraic comparison of numbers in the MNS based on the representation of the compared numbers $S_{MNS} = (s_1, s_2, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_n)$ in AF, i.e. $S'_{MNS} = (s'_1, s'_2, \dots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \dots, t'_n)$. In this case, the following algorithm for comparing two numbers is implemented $S'_{MNS} = (s'_1, s'_2, \dots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \dots, t'_n)$ in the MNS:

$$\left\{ \begin{array}{l} S'_{MNS} = T'_{MNS}, \text{ if } \{(n_{s'} = n_{t'}) \wedge [(s'_1 + t'_1) = 0 \pmod{2}]\}; \\ S'_{MNS} > T'_{MNS}, \text{ if } \{(n_{s'} > n_{t'}) \vee \{(n_{s'} = n_{t'}) \wedge [(s'_1 = 1) \wedge (t'_1 = 0)]\}\}; \\ S'_{MNS} < T'_{MNS}, \text{ if } \{(n_{s'} < n_{t'}) \vee \{(n_{s'} = n_{t'}) \wedge [(t'_1 = 1) \wedge (s'_1 = 0)]\}\}. \end{array} \right. \quad (1.4)$$

The initial numbers S_{MNS} and T_{MNS} are presented in the AF:

$$\left\{ \begin{array}{l} S'_{MNS}(T'_{MNS}) = \frac{D}{2} + |S_{MNS}|(|T_{MNS}|), \text{ if } S_{MNS}(T_{MNS}) \geq 0, \\ S'_{MNS}(T'_{MNS}) = \frac{D}{2} - |S_{MNS}|(|T_{MNS}|), \text{ if } S_{MNS}(T_{MNS}) < 0, \end{array} \right. \quad (1.5)$$

i.e. for positive numbers have that $S'_{MNS} = D/2 + |S_{MNS}|$, and for negative numbers have that $S'_{MNS} = D/2 - |S_{MNS}|$. To determine the result of the operation of comparing two numbers in the MNS, the following obvious relations are used:

$$\left\{ \begin{array}{l} \text{if } S'_{MNS} = T'_{MNS}, \text{ then } S_{MNS} = T_{MNS}, \\ \text{if } S'_{MNS} > T'_{MNS}, \text{ then } S_{MNS} > T_{MNS}, \\ \text{if } S'_{MNS} < T'_{MNS}, \text{ then } S_{MNS} < T_{MNS}. \end{array} \right. \quad (1.6)$$

Let's look at an example for this method of algebraic comparison of numbers in the MNS.

Example 2. Let $S = -2$ ($S_{MNS} = (0, 10, 010)$) and $T = -3$ ($T_{MNS} = (1, 00, 011)$). $S'_{MNS} = D/2 - S_{MNS} = (1, 00, 000) - (0, 10, 010) = (1, 01, 011)$ and $T'_{MNS} = D/2 - T_{MNS} = (1, 00, 000) - (1, 00, 011) = (0, 00, 010)$. By the value of $s'_i = 1$ number $S'_{MNS} = (1, 01, 011)$ choose a constant $NC_{m_i}^{(s'_i)} = (1, 01, 001)$. The adder implements the operation $S''_{m_i} = S'_{MNS} - NC_{m_i}^{(s'_i)} = (1, 01, 011) - (1, 01, 001) = (0, 00, 010)$. By the value of $t'_i = 0$ number $T'_{MNS} = (0, 00, 010)$ choose a constant $NC_{m_i}^{(t'_i)} = (0, 00, 000)$. The adder implements the operation $T''_{m_i} = T'_{MNS} - NC_{m_i}^{(t'_i)} = (0, 00, 010) - (0, 00, 000) = (0, 00, 010)$. Because $S''_{m_i} - n_s \cdot m_i = 12 - 6 \cdot 2 = 0$ and $T''_{m_i} - n_r \cdot m_i = 12 - 6 \cdot 2 = 0$, then for S'_{MNS} and T'_{MNS} the SLBC identical and equal $K_{N_{m_i}}^{(n_{s'})} = K_{15}^{(6)} = \{111111110111111\}$, where $N_{m_i} = 15$ and $n_{s'} = n_{r'} = 6$. When $(n_{s'} = n_{r'})$ the inequality is performed $S'_{MNS} > T'_{MNS}$. In accordance with the relation (1.6) have the result of the comparison operation $S_{MNS} > T_{MNS}$. Check: $S = -2 > T = -3$.

1.5 IMPROVING THE METHOD OF FAST COMPARISON OF TWO INTEGERS IN THE MNS

Obviously, the main disadvantage of all the considered methods is the insufficient accuracy of data comparison, so it is necessary to improve the above methods of comparison. In order to ensure the process of accurate comparison of numbers in the MNS, the method of comparing two numbers has been improved.

As previously noted, the most important characteristic of the process of comparing numbers is the accuracy of comparison W_{m_i} . In the case of comparing numbers in the MNS, the comparison accuracy W_{m_i} two numbers $S_{MNS} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_{i-1}, t_i, t_{i+1}, \dots, t_n)$ depends on the location of the intervals $[g_1 m_i, (g_1 + 1) m_i)$ and $[g_2 m_i, (g_2 + 1) m_i)$ finding these numbers on the axis $0 \div D$, i.e. from numbers g_1 and g_2 these intervals.

When $g_1 \neq g_2$, the algorithm for comparing two numbers S_{MNS} and T_{MNS} is as follows. If $g_1 > g_2$, then $S_{MNS} > T_{MNS}$, what if $g_1 < g_2$ then $S_{MNS} < T_{MNS}$.

When $g_1 = g_2 = g$ the comparison accuracy W_{m_i} depends on the size of the interval $[g m_i, (g + 1) m_i)$, i.e. from the value of the quantity m_i MNS module. For this case $g_1 = g_2 = g$, $S_{m_i} = T_{m_i} = g \cdot m_i$ it's believed that $S_{MNS} = T_{MNS}$. However, this is not always true.

Based on the geometric interpretation (**Fig. 1.5**) of the proposed method for an arbitrary module m_i of the MNS, it's obvious that the comparison accuracy W_{m_i} depends on the size of the interval $[g m_i, (g + 1) m_i)$, i.e. on the value of the module in accordance with which the SLBC was formed. In this case, the comparison accuracy in the MNS can be determined by the following expression:

$$W_{m_i} = \frac{1}{m_i}. \tag{1.7}$$

However, in the case $m_i = m_n$ number of equipment N_{m_i} devices for comparing two numbers S_{MNS} and T_{MNS} , depending mainly on the number of two groups of adders included

in it that implement the operations $S_{m_n} - K_S \cdot m_n = Z_{K_S}^{(S)}$ and $T_{m_n} - K_T \cdot m_n = Z_{K_T}^{(T)}$, is defined by the expression:

$$N_{m_n} = \prod_{k=1}^{n-1} m_k. \quad (1.8)$$

For an arbitrary value m_i of the MNS module, expression (1.8) will have the following form:

$$N_{m_i} = \prod_{\substack{k=1; \\ k \neq i}}^{n-1} m_k. \quad (1.9)$$

Depending on the value of the module m_i , let's consider variants of the method of arithmetic comparison of numbers in the MNS.

Let $m_i = m_n = \max$. In this case, the comparison accuracy W_{m_n} determined by the value of the interval $[gm_n, (g+1)m_n)$ and will be minimal. At the same time, the amount of equipment of the comparing device N_{m_n} (see expression (1.9)) will be minimal. Let $m_i = m_1 = \min$. In this case, for the ordered MNS, the maximum comparison accuracy is provided, which is determined by the value of the interval $[gm_1, (g+1)m_1)$. In this case, the number of equipment devices for arithmetic comparison of two numbers S_{MNS} and T_{MNS} in the MNS maximum and equal $N_{m_1} = \prod_{k=2}^n m_k = m_2 \cdot m_3 \dots m_{n-1} \cdot m_n$.

For MNS, the minimum base is $m_1 = 2$ and the maximum comparison accuracy will be equal to two units, which does not allow achieving the maximum comparison accuracy equal to one (see expression (1.7)).

Thus, it is necessary to improve the methods of arithmetic and algebraic comparison of numbers in the MNS in such a way that the result of comparing numbers in the MNS is determined with maximum accuracy $W_{\max} = 1$ and, preferably, with a minimum number of equipment N_{\min} . The last condition is provided by the choice of base $m_i = m_n = \max$, since it satisfies the conditions N_{\min} .

To improve the method of comparing two numbers in the MNS, which provides the implementation of the functional $F_{opt} = W_{\max}(N_{\min})$, two contradictory conditions must be met. The first, main condition – ensuring the maximum accuracy of comparison is satisfied by choosing the minimum $m_i = \min$ (for example, $m_i = 2$) from the bases of the MNS (**Fig. 1.8**).

However, in this case, the number of device equipment N_{\min} for comparing two numbers S_{MNS} and T_{MNS} will be maximum (see expressions (1.9)). The second condition is to ensure the minimum number of equipment N_{\min} , provided by choosing the maximum $m_i = \max$ base of the MNS.

To eliminate the above contradictions, let's introduce an additional procedure for comparing immediate residuals s_n and t_n initial numbers S_{MNS} and T_{MNS} by base m_n . In this case, the maximum accuracy of the comparison up to unit interval is achieved. So, as a positional comparison of residuals s_n and t_n are carried out in parallel in time with the formation of the SLBC, then the speed of comparing two numbers doesn't decrease.

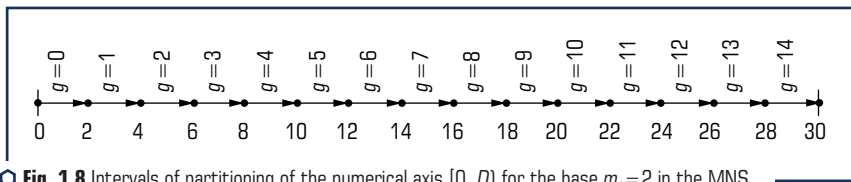


Fig. 1.8 Intervals of partitioning of the numerical axis $[0, D]$ for the base $m_1=2$ in the MNS

Knowing the quantities s_n , t_n , n_S and n_T , mathematical procedure for comparing two numbers $S_{MNS} = (s_1, s_2, \dots, s_{j-1}, s_j, s_{j+1}, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_{j-1}, t_j, t_{j+1}, \dots, t_n)$ in the MNS can be represented as (1.10)–(1.12):

$$S_{MNS} = T_{MNS}, \text{ if } [(n_S = n_T) \wedge (s_n = t_n)]; \quad (1.10)$$

$$S_{MNS} > T_{MNS}, \text{ if } \{(n_S > n_T) \vee [(n_S = n_T) \wedge (s_n > t_n)]\}; \quad (1.11)$$

$$S_{MNS} < T_{MNS}, \text{ if } (n_S < n_T) \vee [(n_S = n_T) \wedge (s_n < t_n)]. \quad (1.12)$$

Improvements to the method for comparing two numbers S_{MNS} and T_{MNS} in the MNS consists in performing the following steps of the algorithm:

1. Representation of compared numbers in the MNS:

$$S_{MNS} = (s_1, s_2, \dots, s_{j-1}, s_j, s_{j+1}, \dots, s_n)$$

and

$$T_{MNS} = (t_1, t_2, \dots, t_{j-1}, t_j, t_{j+1}, \dots, t_n) \text{ in the MNS.}$$

2. Formation by values s_n and t_n of nulling constants of the species:

$$NC_{m_n}^{(S)} = (s'_1, s'_2, \dots, s'_{j-1}, s_j, s'_{j+1}, \dots, s'_n)$$

and

$$NC_{m_n}^{(T)} = (t'_1, t'_2, \dots, t'_{j-1}, t_j, t'_{j+1}, \dots, t'_n).$$

Simultaneously in time, the residuals are compared s_n and t_n compared numbers:

$$S_{MNS} = (s_1, s_2, \dots, s_{j-1}, s_j, s_{j+1}, \dots, s_n)$$

and

$$T_{MNS} = (t_1, t_2, \dots, t_{j-1}, t_j, t_{j+1}, \dots, t_n).$$

3. Determining the values of the difference of numbers S_{m_n} and T_{m_n} :

$$\begin{aligned} S_{m_n} &= S_{MNS} - NC_{m_n}^{(S)} = (s_1, s_2, \dots, s_{i-1}, s_i, s_{i+1}, \dots, s_n) - (s'_1, s'_2, \dots, s'_{i-1}, s'_i, s'_{i+1}, \dots, s'_n) = \\ &= (s_1^{(1)}, s_2^{(1)}, \dots, s_{i-1}^{(1)}, 0, s_{i+1}^{(1)}, \dots, 0) \end{aligned}$$

and

$$\begin{aligned} T_{m_n} &= T_{MNS} - NC_{m_n}^{(T)} = (t_1, t_2, \dots, t_{j-1}, t_j, t_{j+1}, \dots, t_n) - (t'_1, t'_2, \dots, t'_{j-1}, t'_j, t'_{j+1}, \dots, t'_n) = \\ &= (t_1^{(1)}, t_2^{(1)}, \dots, t_{j-1}^{(1)}, 0, t_{j+1}^{(1)}, \dots, 0). \end{aligned}$$

4. Definition of the SLBC components $z_j^{(S)}$ and $z_g^{(T)}$:

$$K_{N_{m_n}}^{(n_S)} = \left\{ Z_{N_{m_n}-1}^{(S)} Z_{N_{m_n}-2}^{(S)} \dots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)} \right\}$$

and

$$K_{N_{m_n}}^{(n_T)} = \left\{ Z_{N_{m_n}-1}^{(T)} Z_{N_{m_n}-2}^{(T)} \dots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)} \right\}.$$

By means of adders, using a set of constants $(0, m_n, \dots, (N-1) \cdot m_n)$ by formulas $S_{m_n} - K_S \cdot m_n = Z_{K_S}^{(S)}$ and $T_{m_n} - K_T \cdot m_n = Z_{K_T}^{(T)}$ components are defined $z_j^{(S)}$ and $z_g^{(T)}$.

5. Formation of quantitative values of PFNC n_S and n_T . By type of the SLBC:

$$K_{N_{m_n}}^{(n_S)} = \left\{ Z_{N_{m_n}-1}^{(S)} Z_{N_{m_n}-2}^{(S)} \dots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)} \right\}$$

and

$$K_{N_{m_n}}^{(n_T)} = \left\{ Z_{N_{m_n}-1}^{(T)} Z_{N_{m_n}-2}^{(T)} \dots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)} \right\}$$

the values of the binary digits of the SLBC are determined for which $z_{n_S}^{(S)} = 0$ and $z_{n_T}^{(T)} = 0$.

6. Implementation of the comparison operation result algorithm S_{MNS} and T_{MNS} :

$$S_{MNS} = T_{MNS}, \text{ if } [(n_S = n_T) \wedge (s_n = t_n)];$$

$$S_{MNS} > T_{MNS}, \text{ if } (n_S > n_T) \vee [(n_S = n_T) \wedge (s_n > t_n)];$$

$$S_{MNS} < T_{MNS}, \text{ if } (n_S < n_T) \vee [(n_S = n_T) \wedge (s_n < t_n)].$$

In accordance with the improved method, **Table 1.7** presents an algorithm for arithmetic comparison of numbers in the MNS.

In order to ensure the process of accurate comparison of numbers $S_{MNS} = (s_1, s_2, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_n)$ in the MNS, presented in AF, based on the method presented in **Fig. 1.8**, improved method of comparing two numbers $S'_{MNS} = (s'_1, s'_2, \dots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \dots, t'_n)$.

● **Table 1.7** Algorithm for arithmetic comparison of numbers in the MNS

No.	Number comparison result	Condition for performing comparison operations
1	$S_{MNS} = T_{MNS}$	$(n_s = n_t) \wedge (s_n = t_n)$
2	$S_{MNS} > T_{MNS}$	$(n_s > n_t) \vee [(n_s = n_t) \wedge (s_n > t_n)]$
3	$S_{MNS} < T_{MNS}$	$(n_s < n_t) \vee [(n_s = n_t) \wedge (s_n < t_n)]$

An improved method for comparing two numbers $S'_{MNS} = (s'_1, s'_2, \dots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \dots, t'_n)$ is based on the representation of numbers in the AF. The improvement of the method of comparing two numbers in the MNS is suitable for both arithmetic comparison and algebraic comparison of data when introducing a sign in an implicit form (representing data in the AF).

An improved method of comparing two numbers in the MNS, presented in the AF consists in performing the following steps of the algorithm:

1. According to the expressions:

$$\begin{cases} S'_{MNS}(T'_{MNS}) = \frac{D}{2} + |S_{MNS}|(|T_{MNS}|), & \text{if } S_{MNS}(T_{MNS}) \geq 0, \\ S'_{MNS}(T'_{MNS}) = \frac{D}{2} - |S_{MNS}|(|T_{MNS}|), & \text{if } S_{MNS}(T_{MNS}) < 0, \end{cases}$$

initial numbers $S_{MNS} = (s_1, s_2, \dots, s_n)$ and $T_{MNS} = (t_1, t_2, \dots, t_n)$ are presented in the AF in the form $S'_{MNS} = (s'_1, s'_2, \dots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \dots, t'_n)$.

2. An algorithm for comparing two numbers is implemented $S'_{MNS} = (s'_1, s'_2, \dots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \dots, t'_n)$ in the MNS as:

$$\begin{cases} S'_{MNS} = T'_{MNS}, & \text{if } \{(n_{s'} = n_{t'}) \wedge [(s'_1 + t'_1) = 0(\text{mod}2)]\}; \\ S'_{MNS} > T'_{MNS}, & \text{if } \{(n_{s'} > n_{t'}) \vee \{(n_{s'} = n_{t'}) \wedge [(s'_1 = 1) \wedge (t'_1 = 0)]\}\}; \\ S'_{MNS} < T'_{MNS}, & \text{if } \{(n_{s'} < n_{t'}) \vee \{(n_{s'} = n_{t'}) \wedge [(s'_1 = 1) \wedge (t'_1 = 0)]\}\}. \end{cases}$$

3. Determining the result of the operation of comparing two numbers in the MNS:

if $S'_{MNS} = T'_{MNS}$, then $S_{MNS} = T_{MNS}$,

if $S'_{MNS} > T'_{MNS}$, then $S_{MNS} > T_{MNS}$,

if $S'_{MNS} < T'_{MNS}$, then $S_{MNS} < T_{MNS}$.

The improved quick comparison method allows to carry out the comparison procedure in the MNS, both in positive and negative numerical ranges. Improving the method of quick comparison

of two integers is carried out by increasing the accuracy of the comparison, by representing numbers in an artificial form, which expands the area of effective use of the CSPIED in the MNS.

The article discusses methods for fast arithmetic comparison of two numbers in the MNS, which are based on obtaining and using PFNC numbers presented in the AF. The use of existing methods for quick comparison of data in the MNS for one-byte, two-byte, three-byte, four-byte and eight-byte numerical bit grids of the CSPIED, respectively, by 16 %, 37 %, 50 %, 58 % and 72 % more efficient in terms of number comparison time than using the fastest of the existing number comparison methods in the MNS, which is based on the principle of nulling.

Designed the method for quick comparison of two integers in the MNS, both in positive and negative numerical ranges, was improved by representing numbers in an artificial form, based on the use of PFNC, which increases the accuracy of comparing numbers in the system of residual classes. The proposed method provides maximum comparison accuracy with a minimum amount of equipment for comparing devices. This circumstance makes it possible to obtain a reliable result of the operation of checking two numbers in the MNS. Based on the developed methods, data comparison algorithms were obtained, in accordance with which devices for their implementation were synthesized. The technical devices, for which patents of Ukraine has been received, is recommended for use in the practical implementation of the CSPIED, which functions as a MNS [3, 10].

The types and methods of cyberattacks are growing exponentially every day, so it is very important to use effective methods and methods of protection. A very important element of various cyberattack detection systems is the data monitoring process, which consists of various methods and algorithms for comparing data. The above method of data comparison for threat detection provides many advantages, but one of the most important is the ability to quickly detect attacks at an early stage and take corrective measures to contain the attacks.

CONCLUSIONS

Based on the conducted research, it is legitimate to draw the following conclusions.

1. In the terms of the development of cyber terrorism in the world, the deployment of cyber-war against Ukraine by the Russian Federation as a component of direct military aggression, there is an increase in risks and threats to cybersecurity. The increase in the number of cyberattacks on critical infrastructure objects and state information resources confirms the urgency of the problem of increasing the cyber resilience of the national information space.
2. Taking into account the growth of negative financial consequences from the implementation of cyber threats, the need to implement comprehensive and coordinated measures at the national and international levels to prevent the implementation of cyber incidents by authorities, businesses and society has been proven.
3. Based on the study of Ukraine's positions in international cybersecurity rankings and the establishment of indicators that are the basis of the global NCSI, GCI and NCPI indexes,

the country's cyber capability strengths and weaknesses are substantiated. Promising tasks are defined as improvement of information protection systems of critical infrastructure objects based on best global practices, as well as coordination of actions with international organizations regarding countering threats related to the development of the digital economy and information society.

4. The formation of a preventive mechanism for combating threats in cyberspace requires a significant increase in the speed and reliability of economic data processing, which is possible based on the use of new machine arithmetic. In this aspect, the proposed non-positional number system in residual classes is one of the promising methods of improving the cybersecurity of critical infrastructure objects, as it enables detecting cyberattacks in the early stages and taking preventive measures to contain them.

5. As a result, the method for quick comparison of two integers in the MNS, both in positive and negative numerical ranges, was improved by representing numbers in an artificial form, based on the use of a positional features of a non-positional code, which increases the accuracy of comparing numbers in the system of residual classes. The proposed method provides maximum comparison accuracy with a minimum amount of equipment for comparing devices. This circumstance makes it possible to obtain a reliable result of the operation of checking two numbers in the MNS. Based on the developed methods, data comparison algorithms were obtained, in accordance with which devices for their implementation were synthesized. The technical device, for which a patent of Ukraine has been received, is recommended for use in the practical implementation of the CSPIED, which functions as a MNS. The above method of data comparison for threat detection provides many advantages, but one of the most important is the ability to quickly detect attacks at an early stage and take corrective measures to contain the cyberattacks.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Yusif, S., Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, 16 (4), 490–513. doi: <https://doi.org/10.1080/19361610.2021.1918995>
2. Protection of information and cyberspace (2022). SIEM report. Security Service of Ukraine. Available at: <http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky>

3. Vlasenko, A. M., Krasnobaev, V. A., Yanko, A. S., Koshman, S. O., Rassomakhin, S. G., Lavrovska, T. V. (2016). Pat. No. 112731 UA. Prystrii dlia kontroliu ta diahnostyky danykh, shcho predstavleni u systemi zalyshkovykh klasiv. MPK: G06F 11/08 (2006.01). No. a201510904; declared: 10.03.2016; published: 10.10.2016, Bul. No. 19. Available at: <https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=227851>
4. Devanny, J., Martin, C., Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, 6 (3), 429–450. doi: <https://doi.org/10.1080/23738871.2021.2000628>
5. Slayton, R. (2020). Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. *Science, Technology, & Human Values*, 46 (1), 81–111. doi: <https://doi.org/10.1177/0162243919901159>
6. Collins, M. (2017). *Network Security Through Data Analysis: From Data to Action*. O'Reilly Media, Inc.
7. Goh, Z. H., Hou, M., Cho, H. (2022). The impact of a cause–effect elaboration procedure on information security risk perceptions: a construal fit perspective. *Journal of Cybersecurity*, 8 (1). doi: <https://doi.org/10.1093/cybsec/tyab026>
8. Liu, J., Yan, J., Jiang, J., He, Y., Wang, X., Jiang, Z. et al. (2022). TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network. *Cybersecurity*, 5 (1). doi: <https://doi.org/10.1186/s42400-022-00110-3>
9. Krasnobayev, V., Kuznetsov, A., Yanko, A., Koshman, S., Zamula, A., Kuznetsova, T. (2019). *Data processing in the system of residual classes*. ASC Academic Publishing.
10. Krasnobaev, V. A., Koshman, S. O., Yanko, A. S. (2014). Pat. No. 92069 UA. Prystrii dlia aryfmetrychnoho ta algebraichnoho porivniannia dvokh chysel klasu lyshkiv. MPK: G06F 7/04 (2006.01). No. u201402480; declared: 12.03.2014; published: 25.07.2014, Bul. No. 14. Available at: <https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=203104>
11. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. *International Journal of Engineering & Technology*, 7 (3.2), 447–452. doi: <https://doi.org/10.14419/ijet.v7i3.2.14569>
12. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine (2022). Microsoft Corporation. Available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>
13. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2022). Increasing Information Protection in the Information Security Management System of the Enterprise. *Proceedings of the 3rd International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 181*. Cham: Springer, 725–738. doi: https://doi.org/10.1007/978-3-030-85043-2_67
14. Shchodo kiberatak na saity derzhavnykh orhaniv (2022). The Security Service of Ukraine. Available at: <https://ssu.gov.ua/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv>
15. Politsiia rozpochala kryminalne provadzhenia za faktom kiberatak na saity derzhavnykh orhaniv (2020). The Cyber Police Department of the National Police of Ukraine. Available at:

<https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/>

16. The State Service for Special Communications and Information Protection of Ukraine. Available at: <https://cjp.gov.ua/ua>
17. Karpenko, O. (2022). USA: The special services of the Russian Federation are involved in DDoS attacks on Ukrainian websites. National Security Council of USA. Available at: <https://ain.ua/2022/02/19/do-ddos-atak-prychetni-speczsluzhby-rf/>
18. Government response: UK assesses Russian involvement in cyberattacks on Ukraine (2022). The UK's National Cyber Security Centre. Available at: <https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine>
19. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. (2020). Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management*, 11 (12), 1709–1726. doi: <https://doi.org/10.34218/ijm.11.12.2020.157>
20. Center for Internet Security. Available at: <https://www.cisecurity.org/>
21. Year in Review: What 2021 Was Like for Cyber Security (2022). Company ESET. Available at: <https://eset.ua/ua/news/view/933/itogi-goda-kakim-byl-2021-dlya-kiberbezopasnosti>
22. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). *The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering Vol. 299*. Cham: Springer, 791–803. doi: https://doi.org/10.1007/978-3-031-17385-1_67
23. The new global cybersecurity index is the National Cyber Power Index (2020). The official website of the Public Organization "International University of Cyber Security". Available at: https://www.icu-ng.org/icu-ng/novyny/novyj-globalnyj-indeks-kiberbezpeky-nacjonalnyj-indeks-kiberpotuzhnosti/#_ftn1
24. Cyber security management best practices. Review report (2022). Committee on Digital Transformation. Available at: https://www1.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_04.pdf
25. NCSI Project Team. Available at: <https://ncsi.ega.ee/country/ua/>
26. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro nevidkladni zakhody z kiberoborony derzhavy". Ukaz Prezydenta Ukrainy No. 446/2021. 26.08.2021. Available at: <https://zakon.rada.gov.ua/laws/show/446/2021#Text>
27. Glushko, A. D. (2013). Directions of Efficiency of State Regulatory Policy in Ukrain. *World Applied Sciences Journal*. Pakistan: International Digital Organization for Scientific Information, 27 (4), 448–453.
28. Diogenes, Y., Ozkaya, E. (2019). *Cybersecurity Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals*. Packt Publishing Ltd.

29. Bosilca, G., Delmas, R., Dongarra, J., Langou, J. (2009). Algorithm-based fault tolerance applied to high performance computing. *Journal of Parallel and Distributed Computing*, 69 (4), 410–416. doi: <https://doi.org/10.1016/j.jpdc.2008.12.002>
30. Hlushko, A., Yanko, A. (2019). Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. *Economics and Region*, 4 (75), 35–44. doi: [https://doi.org/10.26906/eir.2019.4\(75\).1814](https://doi.org/10.26906/eir.2019.4(75).1814)
31. Krasnobaev, V. A., Kurchanov, V. N., Yanko, A. S. (2015). Method of quick comparison of two integers in the system of final classes. *Problems of Informatization*. Cherkasy, 45.

CHAPTER 2

**ECONOMIC CYBER SECURITY OF BUSINESS IN UKRAINE:
STRATEGIC DIRECTIONS AND IMPLEMENTATION MECHANISM****ABSTRACT**

The study is devoted to the determination of strategic directions for ensuring the economic cyber security of business in Ukraine. The importance of information protection in the context of the development of the digital economy has been updated. The place of economic cyber security in the national security system is determined. A thorough analysis of the dynamics of cyber incidents in the world in recent years has been conducted. The specifics of the manifestation of cyber threats at the macro and micro levels are outlined. Qualitative changes in the state policy of Ukraine in the aspect of ensuring information and cyber security have been studied. A number of the most relevant risks and threats to the economic cyber security of business in 2023 have been identified. The need for business entities to develop an effective internal policy of cyber protection of computer networks against attacks, intrusions and unauthorized access is proven. The modern trends of cyber threats are studied and the cyber security policy strategy of business entities in Ukraine is described.

Special attention is paid to the intrusion detection process. The working principles of modern intrusion detection and prevention systems have been studied in detail. Behavioral analytics of UEBA users and objects were considered to detect violations in the field of security. On the basis of Microsoft's Advanced Threat Analytics (ATA), the process of monitoring network traffic of domain controllers was considered, with the aim of detecting cyber-attacks. Using Azure Security Center as an example, it explores intelligent security tools and expanding analytics to detect threats faster and reduce the number of false security alerts. Using the proposed cybersecurity policy recommendations will significantly increase the level of business information security (confidentiality, integrity, and availability).

KEYWORDS

Economic cyber security, information security, national economy, business, cyber security infrastructure, computer network, intrusion detection systems, unauthorized access, intrusion prevention system, cyber security strategy, security center.

The global processes of information technology development have become a determinant of the development of the digital economy and a powerful tool for global economic growth. On the one hand, the digitalization of all spheres of public life allowed maximizing the benefits of the state, business and citizens in connection with increasing the efficiency and effectiveness of operations, information exchange, but on the other hand, it caused an increase in risks associated with receiving financial and reputational losses as a result of cybercriminal activities. The urgency of the problem of protecting cyberspace in the context of the development of artificial intelligence systems is due to the growth of cyber incidents both in the national and in the global information space. Interference and destabilization of information systems, theft of confidential information are cyber threats that are modified every day and require business entities to build effective protection systems. In this regard, the need to develop a cyber security policy and a mechanism for its implementation at the micro level, which will minimize cyber security risks for business in Ukraine, is gaining indisputable relevance.

The research was supported by the Ministry of Education and Science of Ukraine and performed the results of the project O122U001749 "The formation of organizational and economic principles for the prevention of threats to the social and economic security of Ukraine in the conditions of a pandemic".

2.1 RISKS AND THREATS TO ECONOMIC CYBER SECURITY OF BUSINESS

The development of the digital economy in recent decades is a strategic direction of the world's leading countries. In this regard, the current stage of society's development is characterized by the integration of security aspects of economic and information processes, which requires the transition of the management system at both the macro and micro levels to a qualitatively new level.

The digital economy is a type of economy in which digital data are the key factors of production. Their use as a resource makes it possible to significantly increase the efficiency, productivity, value of services and goods, to build a digital society.

To date, the size of the digital economy, according to various estimates, is from 15.5 % to 17.5 % of world GDP. Almost 40 % of the added value created in the global sector of information and communication technologies is accounted for by the United States and China. It is predicted that by 2030 the share of the digital economy in the GDP of the world's largest countries will reach 50–60 % [1, 2].

One of the indicators that characterizes the development of the digital economy is the International Digital Economy and Society Index (I-DESI), which is based on a comparative analysis of the digital efficiency indicators of EU member states and 19 other countries of the world (Australia, Albania, Bosnia and Herzegovina, Brazil, Canada, Chile, Iceland, Israel, Japan, Mexico, Montenegro, North Macedonia, Norway, Serbia, South Korea, Switzerland, Turkey, United Kingdom, and the United States) [3]. According to the results of 2022, the EU-27 member states are in the first five positions out of the 10 TOP in the I-DESI index. Overall index scores remain higher for non-EU

countries than for EU-27 member states in each year. Denmark had the highest I-DESI score. It was also the leading country in the EU according to the 2021 DESI index. Iceland became the leading country outside the EU (Fig. 2.1).

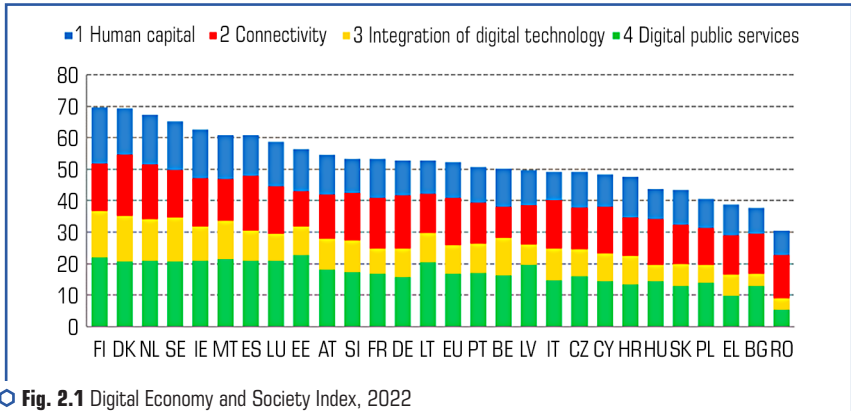


Fig. 2.1 Digital Economy and Society Index, 2022

Note: compiled by the authors according to [4]

In general, in developed countries, the level of cyber security and indicators of the development of the digital economy are on average higher than in developing countries.

Regarding the level of digitization of the economy of Ukraine, it is possible to note a significant difference in various industries. In particular, in the field of financial services, communication services, and logistics, national business entities use digital technologies on a par with global competitors [5]. Along with a number of advantages, this creates new risks for Ukrainian business, including threats to cyber security, and requires an appropriate response and a systemic approach from both the state and business entities.

State policy is usually manifested in two main aspects – state support for development (concepts, strategies, doctrines, state programs) and state regulation of relations (legislative acts) [6]. It is appropriate to note that starting from 2021, from the moment of adoption of the Information Security Strategy of Ukraine and the Cyber Security Strategy of Ukraine, the foundations were laid for the development of effective mechanisms for countering threats to the national economy in the information sphere, including in cyberspace. The information security strategy of Ukraine outlines the need to strengthen the capabilities to ensure the information security of the state, its information space, support with information means and measures of social and political stability, state defense, protection of state sovereignty, territorial integrity of Ukraine [7]. The cyber security strategy defines Ukraine's urgent need to ensure socio-economic development in the digital world, which requires the acquisition of the ability to effectively deter destructive actions in cyberspace, the achievement of cyber resilience at all levels, and the interaction of all cyber security actors [8].

Taking into account the provisions of the strategies and other legal acts, it is legitimate to outline the place of cyber security of the economic sphere in the national security system (**Fig. 2.2**).

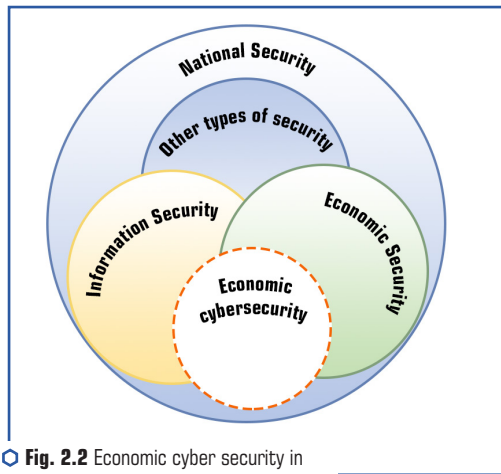


Fig. 2.2 Economic cyber security in the national security system

Therefore, national security must be considered taking into account the processes of digitalization, which have radically changed the paradigm of socio-economic development. The latest economic processes in cyberspace require adequate security measures. Economic cyber security occupies a special place in the national security system, because cybercrimes in the form of cyber espionage (theft of information about the latest technological developments, financial transactions, etc.) and cyber-attacks can cause irreparable damage to strategically important objects of both the public and private sectors. This is confirmed by official static data.

The public sector became the main target for cybercriminals in 2022: the number of attacks on this sector increased by 95 % in the second half of 2022 compared to the same period in 2021 (**Fig. 2.3**).

The increase in digitalization brought about by COVID-19 has not only increased the attack surface for attackers, but has also allowed countries to use cyberwarfare as a tool to attack other countries.

In recent years, India, the USA, Indonesia and China have remained the main target countries for cyber-attacks (**Fig. 2.4**). Together, these four countries account for about 40 % of the total number of public sector incident reports.

The Russian Federation's full-scale invasion of Ukraine was accompanied by coordinated cyber-attacks on state institutions and critical infrastructure facilities. At the same time, the number of cyberattacks against Russia increased by more than 600 % in support of Ukraine by activists.

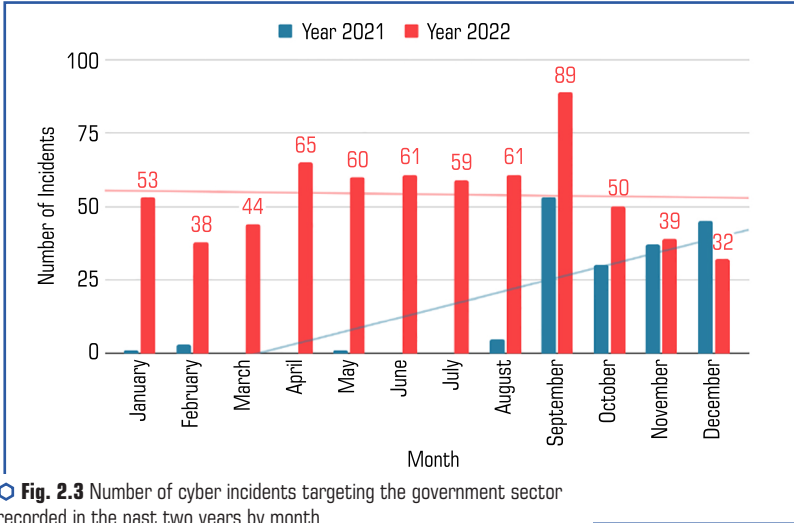


Fig. 2.3 Number of cyber incidents targeting the government sector recorded in the past two years by month

Note: compiled by the authors according to [9, 10]

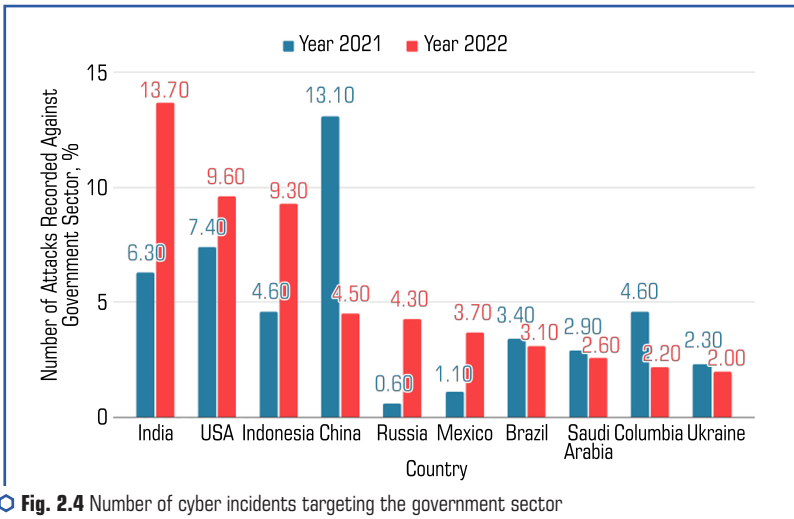


Fig. 2.4 Number of cyber incidents targeting the government sector recorded in the past two years by country

Note: compiled by the authors according to [9, 10]

The high level of development of cyberspace and the organization of cyber threats indicates the need to change the paradigm of cyber security strategy: it should be based not on responding to the

fact, but on the principles of forecasting and planning protection against future actions of cybercriminals. For this, it is necessary to constantly analyze modern trends in economic cyber threats [11].

At the macro level, the most dangerous trend is the use of cyber weapons in conflicts between countries, which is taking on new forms. Cyberactivity plays a leading role in this destructive dialogue. Attacks on critical infrastructure and purposeful destabilization of the Internet in certain countries open a new era of cyber-attacks.

The main cyber threats to business, i.e. the micro level, can rightly be identified as the following:

1. Phishing is one of the most common types of cybercrime, which leads to countless financial losses every year. The goal is to steal sensitive data and credentials, such as login credentials or credit card details, and trick people into allowing malware to be installed.

2. Malware – hackers develop malware to have persistent backdoor access to company devices that is difficult to detect. They can then remotely control the device and use it to steal data, explore the local network, or send spam from the infected device. 91 % of cyber-attacks start with a phishing email, so phishing and malware are closely related.

3. Ransomware – this form of malware can cause catastrophic damage to a business. Ransomware blocks a firm's information system and deprives it of access to critical data until a ransom is paid to return sensitive information and regain control of the systems. Ransomware presents businesses with a difficult choice: pay the attackers or lose data and access to it. Most companies choose to pay hackers, but even when business owners pay the ransom, they don't always get access to their data.

4. Compromise of corporate e-mail (BEC – Business Email Compromise) is one of the most expensive cybercrimes. The process begins with criminals hacking business systems in order to gain access to information about their payment systems. They then deceive employees and encourage them to make payments to bogus bank accounts instead of real ones. Fake payment requests can be difficult to identify because they look almost identical to genuine requests. BEC can result in huge financial losses for a business and it can take months to track down and recover payment amounts, if at all.

5. Internal threats – some of the company's employees have access to confidential information. Whether they are current or former employees, partners or contractors, 25 % of data breaches are caused by insider threats. Unscrupulous employees act out of greed, or sometimes disgruntled employees act out of bitterness. In any case, their dissemination of important information can cause significant financial losses.

6. Inadvertent disclosure – employees may accidentally disclose confidential information and cause financial damage to the company. A mistake could be as simple as accidentally sending an email to everyone in the company. Companies with a large number of employees are at particular risk if employees have access to core databases.

7. Storage intelligence – companies store huge amounts of data in the cloud and believe that it is automatically protected. However, this is not always the case. Cybercriminals look to unsecured cloud storage to access and exploit data. Cloud interfaces are not always supported by

secure systems, making them easy prey for cybercriminals. Probably the most famous example of this is the breach of an unsecured cloud S3 bucket containing vast amounts of classified National Security Agency data. The data was breached in 2017 with serious consequences. Companies should be aware that the storage of confidential information can be risky if appropriate precautions are not taken.

8. Social engineering – involves the creation of fictitious persons and profiles by cybercriminals on social networks in order to gain the trust of their victims and obtain the information necessary to complete the operation. These relationships are used to achieve the ultimate goals of phishing and installing malware to disrupt businesses, gain access to company data, and gain financial gain. Any form of social interaction designed with the ultimate goal of deceiving a business can be classified as social engineering [12, 13].

Fig. 2.5 schematically presents threats to the cyber security of business entities according to the 2022 report on global IT risks from Cisco Talos. The main causes of the most expensive data leaks are related to the mentioned cyber-attacks [14].

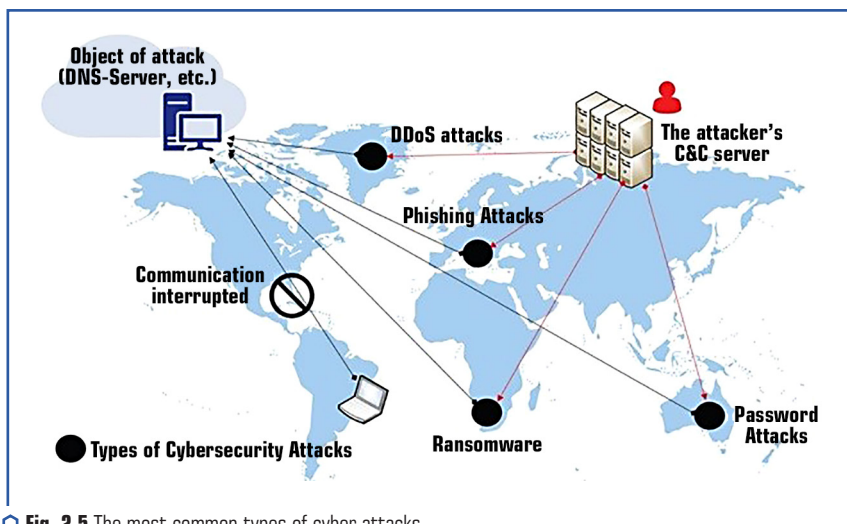


Fig. 2.5 The most common types of cyber attacks

Financial losses from cyber-attacks are difficult to estimate. However, according to approximate estimates of experts, the world economy will experience losses measured in trillions of US dollars. However, the greatest danger is not in the amount of money, but in the threat to the business. So, every fifth company that was subjected to a cyber-attack was forced to close its business. 48 % of companies experienced data or equipment loss, and of the 42 % that paid the ransom, a quarter did not receive the promised data [15].

The outlined risks and threats to the economic security of business require the implementation of effective mechanisms for their prevention and neutralization both at the level of the state [16] and at the level of business entities.

Taking into account the improvement of national legislation in the field of information and cyber security, it should also be noted that in February 2023, the Protective DNS system was implemented in Ukraine. It provides filtering of phishing sites, thus hindering the activities of cybercriminals, and Ukrainians have received additional protection from fraudsters on the Internet. When trying to go to a phishing site, Protective DNS redirects users to a page with a warning about the threat and recommendations on cyber hygiene. More than 320 Ukrainian providers have already joined the system, which are responsible for the security of their customers. Among them are the largest market players – Kyivstar, Lifecell, Vodafone, Ukrtelecom, Datagrup and Volya. In the first month of the system's operation, there are significant results – the volume of phishing fraud in monetary terms fell by approximately 40–50 %, and the number of appeals from defrauded citizens – by 30–40 %. In general, these are tens or even hundreds of millions of hryvnias every month, which Ukrainians will not lose thanks to the operation of the system [17].

Thus, in the aspect of ensuring economic cyber security, it is necessary to establish an exchange of information about cyber incidents and develop close cooperation of the state with scientific institutions and private companies, as well as international organizations. At the same time, at the level of business entities, it is necessary to develop individual cyber security strategies and mechanisms for their implementation.

2.2 CYBER SECURITY POLICY STRATEGY OF BUSINESS OF UKRAINE

The concept of security of any system is a complex concept that can be considered from different aspects and implemented in many ways and methods, but all active actions must be aimed at the constant security of both the system as a whole and its individual elements, which ensures the sustainable development of the system, timely detection, prevention and neutralization of real and potential threats. Today, in the era of digitalization of almost all spheres of the economy, it is necessary to pay special attention to the cyber security policy of economic entities [18]. In modern conditions, the problem of economic cyber security of Ukraine is intensifying in connection with military actions in the country, as well as the activation of European integration processes. This requires a review of existing concepts of cyber security at the level of business entities and improvement of priority ways of ensuring it. Since there are international standards that must be met if it is planned to become part of the EU in the future, for example, in 2016, the European Parliament adopted the General Data Protection Regulation (GDPR) [19]. Starting from the spring of 2018, according to the GDPR, companies are obliged to:

- report information leaks;
- appoint a person responsible for data protection;

- ask for user permission for data processing;
- make the data anonymous to preserve privacy [20].

All organizations operating on the territory of the European Union must comply with these standards.

Business security in the information space is most necessary to be considered from the point of view of protection against various types of attacks and prevention of existing cyber threats, that is, against unauthorized access.

An analysis of current trends shows that over time, hacker attacks have proven to cyber security experts that attackers (hackers) can be persistent, more creative and increasingly sophisticated in their attacks. Attackers have learned to adapt to changes in the IT landscape in order to always act effectively when launching an attack. Although there is no Moore's Law or its equivalent in the context of cyberattacks, it can be said that hacking methods are becoming more sophisticated every year.

In the last few years, there has been a trend towards better attacks and methods of their implementation, therefore the internal information and cyber security policy of any business entity must be effective, flexible and dynamically adapt to existing cyber threats.

According to Verizon's 2022 Information Security Incident Investigation Report, the relationship between a threat actor, their motivations, and their modus operandi varies by industry. Nevertheless, the report states that the main attack vector is the state financial structures and the banking sector. On January 25, specialists of the cyber security company Proofpoint published a detailed analysis of ART TA444, which focuses on financial crimes in the interests of the leadership of North Korea, the main targets of this cyber-attack: banks, financial institutions of many countries around the world, as well as the circulation of cryptocurrencies. Therefore, there is an urgent need for information protection of elements of the economic system of countries, including: websites of state and private economic institutions, network equipment of computer systems, methods of authentication and authorization, etc. Because, as a rule, business entities are focused on profits, and often forget about compliance with cybersecurity policies.

On January 24, the cybersecurity company Cisco Talos released its final report on the state of cybersecurity in 2022. In addition to the pronounced impact of the Russian-Ukrainian cyber confrontation, the company's specialists note several other important trends:

- dual purpose cyber security tools allow malicious actors to remain undetected in the affected environment;
- criminals actively use legitimate utilities/systems (such as PowerShell) for their purposes;
- expanding the scope of using the traditional form of spreading viruses via USB [21].

Guidelines from cybersecurity infrastructures such as the International Organization for Standardization (ISO) 27000 or the National Institute of Standards and Technology (NIST) should be used when creating the cybersecurity policy of economic entities. Many organizations, including Microsoft, are implementing a zero-trust security strategy to protect remote and hybrid workers (network users) who need secure access to company resources from anywhere. But any chosen

cybersecurity policy strategy includes the core functions of protection, detection, response, prevention, and recovery. Based on the main functions of modern cyber security strategies, the main attention should be focused on methods of detecting and preventing intrusions.

Of course, in the issue of protecting the economy from cyberattacks on a national scale, under the conditions of informatization, digitalization, and computerization, it is necessary to consider the economic system at the level of each economic entity [22]. The network of any institution is a complex system of communication between various elements of the economic structure, which is implemented on the basis of computer systems of various functional purposes and network equipment. From the point of view of information security, it is necessary to consider them as a computer network, since most of the existing threats and attacks in cyberspace are carried out precisely from the global Internet network to which all economic structures are connected (Fig. 2.6).

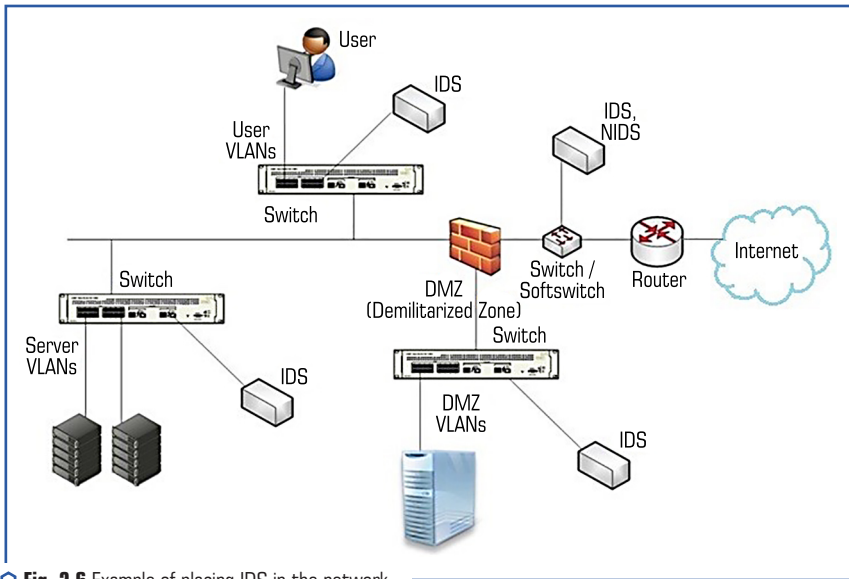


Fig. 2.6 Example of placing IDS in the network

Detection of network attacks is currently one of the most acute problems of the secure use of corporate networks. Large-scale epidemics of network worms, automated means of finding network vulnerabilities – all this makes ensuring the security of local networks of any enterprise a very time-consuming task. Now it is difficult to find a network that does not have such active means of preventing attacks as an antivirus, a brandmauer or a firewall, etc. However, active attack detection tools alone are not enough, because in cyber-attacks of any scale, the attacker scans the

network using specially prepared scripts that identify potentially weak nodes. Selected nodes are attacked, which consists in sending certain bits (packets, frames, etc.), and the attacker gains administrative rights to them. Trojans (again certain types of active data attack prevention tools) are installed on hijacked nodes and run in the background. Therefore, the process of scanning data with the help of certain network scanners and sensors (which are included in the SBB, or are installed separately for additional monitoring) is one of the key factors in protecting against hacker attacks, since hacking mechanisms and all scenarios of cyber-attacks, regardless of their type (DoS, DDoS attacks, etc.) consists first in the possibility of access, and then in the acquisition, blocking, editing or destruction of data. In other words, when attacking a network, hackers send disguised data, usually as service information, which are actually parts of hacking code. Therefore, a very important element of information security of the economic sector is the development of effective monitoring of cyber security system events, which consists primarily of filtering traffic (network data). Currently, there are many information security monitoring systems based on Zabbix, DellFoglight, and Microsoft SCOM, among others, but the algorithm of their actions is well known to criminals, and the hacking of such a system is a matter of time [18].

Based on the above, it is necessary to actively monitor suspicious actions and threats and take action. Any security strategy will not be complete if there is no detection system, which means the presence of the necessary sensors of the intrusion detection system (IDS), which are distributed over the network and monitor actions (**Fig. 2.6**). Cybersecurity professionals must take advantage of today's detection technologies that profile users and computer systems to better understand anomalies and deviations from normal behavior and take preventive measures.

Therefore, the presence of a reliable and effective mechanism for detecting and preventing intrusions, which are the main elements of monitoring, are quite important, as they are one of the tools for building effective information security of financial institutions [23]. That is why this section will consider such questions as:

- detection capabilities;
- intrusion detection systems (IDS – Intrusion Detection System);
- intrusion prevention systems (IPS – Intrusion Prevention System);
- behavioral analytics within the organization;
- behavioral analytics in the hybrid cloud;
- placement of IDS in the network.

Intrusion detection process

The current threat landscape requires a new approach to detection systems that relies on the traditional complexity of fine-tuning initial rules, thresholds, and baselines. Dealing with multiple false positives becomes unacceptable for many organizations. When preparing to defend against attackers, the cybersecurity team should use a number of methods, which include:

- correlation of data from several sources;
- profiling;
- behavioral analytics;

- detection of anomalies;
- assessment of activity;
- machine learning.

It is important to emphasize that some traditional security controls, such as protocol analysis and signature-based antivirus software, still have their niche in the defense line, but are designed to combat legacy threats. Of course, it is not necessary to remove antivirus software that to use just because it doesn't have machine learning capabilities. This is still your host's security level.

On the other hand, the traditional mindset of cyber security professionals, which focuses only on monitoring high-powered users, is over and can no longer be that approach. To identify current threats, it is necessary to view all user accounts, profile them, and understand common behavior. Active threat actors will attempt to compromise the average user, remain on the network, and continue the intrusion through further propagation and privilege escalation. For this reason, there must be detection mechanisms that can identify such behavior across devices, in different locations, and generate alerts based on data correlation, as shown in **Fig. 2.7** [24].

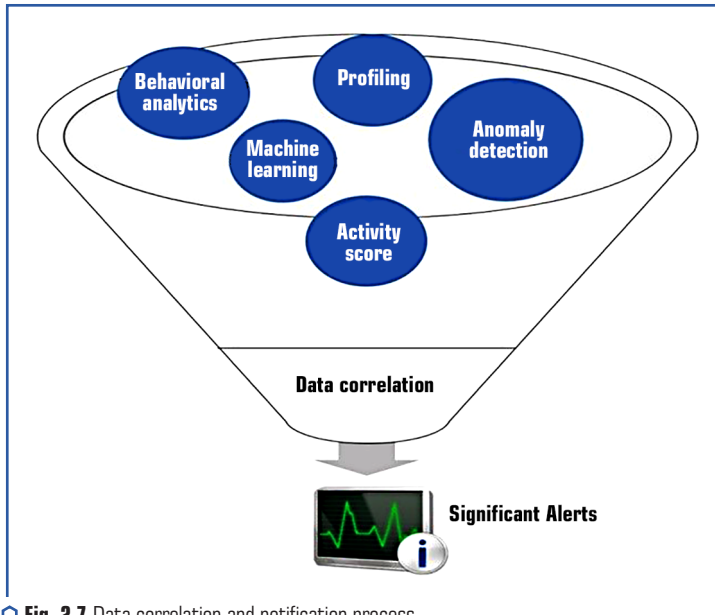


Fig. 2.7 Data correlation and notification process

When data is contextualized, the number of false positives is naturally reduced, which has a significant impact on the security system.

Speaking of detection, it is important to mention indicators of compromise (Indicator of Compromise, IoC). When new threats appear in the natural environment, they usually have some kind of behavioral pattern and leave their mark on the victim's system.

For example, in June 2017, a large-scale cyberattack on various businesses and organizations, including a large number of financial institutions, was carried out using the Petya ransomware [25], which executed the following commands on the target system to reschedule the restart:

```
schtasks /Create /SC once /TN «» /TR «<systemfolder>shutdown.exe /r /f» /ST <time> cmd.
exe /c schtasks /RU «SYSTEM» /Create /SC once /TN «» /TR «C:\Windows\system32\shutdown.exe
/r /f» /ST <time>
```

Another indicator of the activity of this program is the scanning of the local network through TCP ports 139 and TCP 445. These are important signs that the target system is under attack and the culprit is Petya. Discovery systems will be able to collect these indicators of compromise and issue alerts when an attack occurs. Using Azure Security Center as an example, some time after detecting the Petya threat, the center automatically updates its security mechanism and can alert users that their computer has been compromised, as shown in **Fig. 2.8** [24].

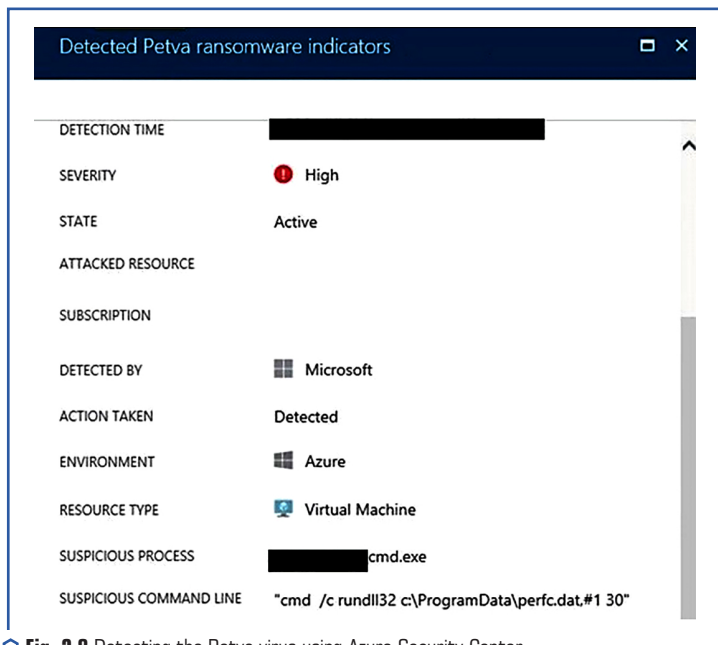


Fig. 2.8 Detecting the Petya virus using Azure Security Center

One of the options for using cyber security infrastructures in this aspect is the possibility to register on the OpenIOC website (<http://openioc.org>) to receive information about new indicators, as well as to contribute to the security of cyberspace based on previous experiences. Using the IoC Editor (see the help section for the URL from which it can be downloaded), it is possible to create your own indicator or browse an existing one. The cyber security team must always be aware of the latest threats and IoC.

Intrusion detection and prevention systems

An intrusion detection system (IDS) is a software or hardware tool designed to detect unauthorized access to or control of a computer system or network (mainly via the Internet). An IDS is one of the most important cyber security considerations that can detect intrusions before and/or after an attack [26]. As the name suggests, IDS is responsible for detecting a potential intrusion and initiating an alert. What can be done with this alert depends on the policy of the detection system [27]. In other words, IDS registers suspicious activities on the network and informs the person responsible for information security about them. Simplified, it can be imagined in the form of the scheme presented in **Fig. 2.9**.

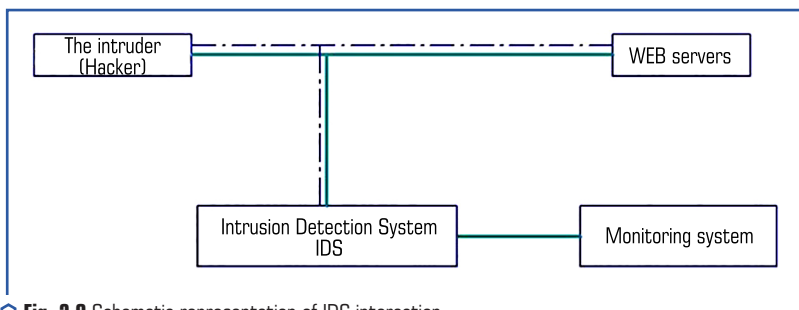


Fig. 2.9 Schematic representation of IDS interaction

When creating an IDS policy, the following step-by-step steps must be taken into account:

- determine those responsible for IDS control and availability of IDS administrator rights;
- determine the procedure for processing incidents based on alerts generated by IDS;
- determine the IDS update policy;
- determine the location of the IDS in the network.

These are just a few examples of the primary steps that should help in planning and implementing an IDS.

There are various variants of IDS classification, for example, IDS can be classified based on their, Detection methods, Deployment method, and Response method [28]. IDS can be divided into: network intrusion detection systems (NIDS) and host-based systems (HIDS) (**Fig. 2.10**).

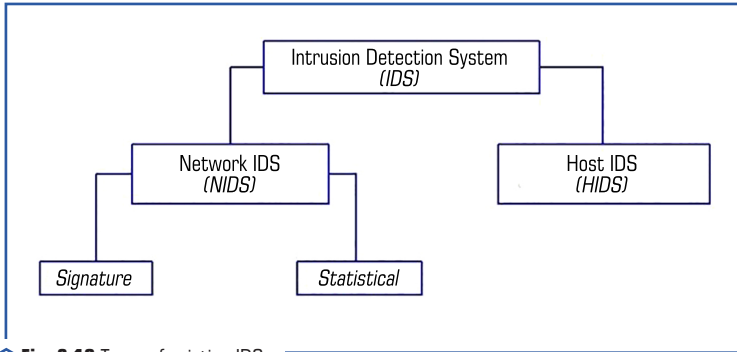


Fig. 2.10 Types of existing IDS

A HIDS node-based system is installed on each computer in the network to analyze and monitor traffic coming to the respective node, and from there HIDS also monitors and controls local file changes and possible changes due to unauthorized access.

NIDS analyzes traffic to detect known attacks based on existing rule sets. NIDS detects intrusions for the network segment in which it is installed. This means that in the case of NIDS, placement becomes critical to garnering valuable traffic. This is where the cybersecurity team must work closely with the IT infrastructure team to ensure IDSs are installed in strategically important locations throughout the network. When planning NIDS placement, prioritize the following network segments:

- Demilitarized Zone (DMZ);
- main corporate network;
- wireless network;
- virtualization network;
- other critical network segments.

Sensors that are part of the NIDS look at network traffic or logs and pass them to analyzers that look for information of a malicious nature in the received data and, in case of successful detection, send the results to the monitoring system. If the network sensors listen (analyze) traffic, that means they won't consume too much network bandwidth. Let's note that in the IDS deployment shown in **Fig. 2.6**, a detection system (which is actually a NIDS in this case) has been added to each segment (using a SPAN port on the network switch).

NIDS, in turn, fall into two broad categories, signature and statistical.

A signature-based intrusion detection system will query a database of signatures (traces) of already known attacks and known system vulnerabilities to check whether what has been detected is a threat and whether an alert should be triggered. Signature methods describe an intrusion using a formal model – it can be a character string, a semantic expression, etc. Signature analysis was the first method used for intrusion detection. This method checks whether the sequences match

the signature. A signature is a signature, a pattern, for example, it can be a characteristic string of a program that indicates malicious traffic. The signature may contain a key phrase or command that is associated with the intrusion. If a match is found, an alarm is raised. The signature method protects against a hacker or virus attack only if its signature (for example, a fragment of the virus body) is known in advance. The advantages of signature intrusion detection methods are low computational complexity and low cost of deployment and application. The disadvantages of signature methods include the low efficiency of detecting unknown attacks and the problem of the aging of signature databases. Since it is the database of these signatures, it requires constant updating to have the latest version available. A behavior-based IDS works by creating basic patterns based on what it learns from the system. By learning normal behavior, it becomes easier to detect deviations.

Statistical methods are widely used to detect anomalies and are based on the construction of a statistical profile of the system's behavior during the training stage. System behavior should be normal during training. Further, for each parameter of the system functioning, it is necessary to form an interval of acceptable values using some known law of probability distribution. Statistical intrusion detection systems use a statistical approach and, after installation, are "learned" by the administrator, who sets the policy of the detection system, corresponding to normal activity in the network – types of traffic, connections between nodes, used protocols and ports. When detecting network intrusions or significant traffic differences from the typical in a particular system, IDS notifies the administrator. The statistical approach is highly sensitive to the correctness of the recognition rules. As a result, if the rules are set incorrectly, the system may trigger a false positive and differ in the complexity of the settings.

An effective IDS must be both signature and statistical, because some attacks have a pronounced signature, while others do not, but they cause deviations in the lower levels of the protocol stack (TCP/IP), which is exactly what a statistical IDS can detect. In wireless networks, the task of detecting intrusions is complicated by radio interference, refraction reflection, and signal scattering.

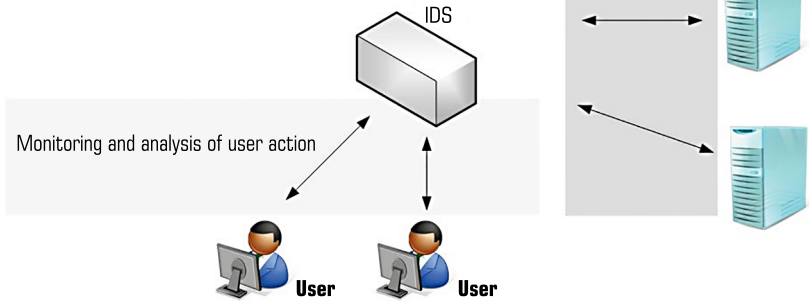
Regardless of the chosen one, a typical IDS has the capabilities shown in **Fig. 2.11**. In addition to the functions of constant monitoring and analysis of what is happening, IDS systems perform the following functions:

- collection and recording of information;
- notification of network administrators about the changes that have occurred;
- creation of reports for summarizing logs.

While these are the basic capabilities, the number of features will actually depend on the vendor of the security tool (software and/or hardware) and the method used by the IDS. The implemented IDS should be based on various detection methods and technologies, as well as flexibly integrated with the general cooperative structure of the enterprise network [29]. IDS has got many developments through its datasets, new technologies and methods but as the technologies increases, the threats of attacking the system and data breaches also increases, so in order to overcome this problem a hybrid framework for the intrusion detection has to be developed to detect the intrusions from the intruder [28].

IDS control panel

- Statistical analysis
- Analysis of anomalous activity
- Pattern analysis



◉ **Fig. 2.11** Scheme of a typical IDS

An Intrusion Prevention System (IPS) uses the same concept as an IDS, but as the name suggests, it prevents intrusions by taking corrective actions. These actions will be debugged by the IPS administrator. It is worth noting that IPS is a subclass of IDS (active IDS) and is therefore based on its attack detection methods. The ability to prevent attacks is realized due to the fact that the network IPS is usually built into the network gap and passes traffic through it further if it is recognized as safe [30]. IPS works, of course, slower than ordinary IDS, because it is necessary to analyze and immediately pass traffic. IPS technology, in turn, in addition to the IDS functions listed above, is able not only to identify the threat and its source, but also to block them. This indicates the extended functionality of such a solution. IPS is able to perform the following actions:

- terminate malicious sessions and prevent access to the most important resources;
- change the configuration of the "protected" environment;
- perform actions on attack tools (for example, delete infected files).

Just as IDS is host-based (HIDS) and network-based (NIDS), IPS is host-based (HIPS) and network-based (NIPS). Placing NIPS on the network is critical, and the same guidelines as previously mentioned apply here. Consideration should also be given to positioning NIPS according to traffic so that corrective actions can be taken if necessary.

IPS can typically operate in one or more of the following modes:

- based on the rules;
- based on the anomalies.

Rule-based detection. When operating in this mode, IPS compares traffic against a set of rules and attempts to verify that the traffic matches the rule. This is very useful when it is necessary to deploy a new rule to block an attempt to exploit vulnerabilities. NIPS systems such as Snort are capable of blocking threats using rule-based detection [30]. For example, the Snort rule Sid 1-42329 is able to detect the Win.Trojan.Doublepulsar variant. Snort rules can be found here: [etc/snort/rules](#), and other rules can be downloaded from the official site.

Sometimes multiple rules are needed to neutralize a threat. For example, rules 42340 (Anonymous SMB session IPC access attempt), 41978 (SMB remote code execution attempt), and 42329-42332 (Win.Trojan.Doublepulsar variant) can be used to detect the Wanna-Cry ransomware.

The advantage of using an open source NIPS such as Snort is that when a new threat becomes available on the network, the community usually reacts quite quickly by publishing a new rule to detect the threat. For example, when the Petya ransomware was discovered, the community created a rule and posted it on GitHub. Although vendors and the security community are really quick to publish new rules, it's still up to cybersecurity professionals to keep an eye out for new indicators of compromise and create NIPS rules based on them.

Anomaly based detection. In this case, the anomaly is based on what the IPS classifies as anomalous. This classification is usually based on heuristics or summation of rules. One of the options is statistical anomaly detection, in which samples of network traffic are taken at random moments of time and a comparison is made with the baseline state. If this sample deviates from the baseline, an alert is triggered with further action.

It is worth noting that the UTM firewall, network sensors and any modern intrusion detection and prevention systems are the optimal combination of IDS and IPS technologies.

The method of detecting malicious activity (malicious activity) as a behavioral and analytical mechanism of cyber security

For the vast majority of companies on the market today, the core business is still conducted within the organization. It's where mission-critical data resides, where most users work, and where key resources reside. There are many attacker attack strategy scenarios, but they all have common steps: infiltrate the local network, spread further, elevate privileges, and maintain communication with the command-and-control server until that server can complete its mission. For this reason, the presence of behavioral analytics is required to quickly break the attack lifecycle [24].

According to Gartner, it is very important to understand how users behave. By monitoring legitimate processes, organizations can use User and Entity Behavior Analytics (UEBA) to detect security breaches. There are many benefits to using UEBA's behavioral analysis system to detect attacks, but one of the most important is the ability to detect attacks at an early stage and take corrective measures to contain the attack.

Fig. 2.12 shows an example of how UEBA looks at different objects to decide whether an intrusion alert should be triggered or not.

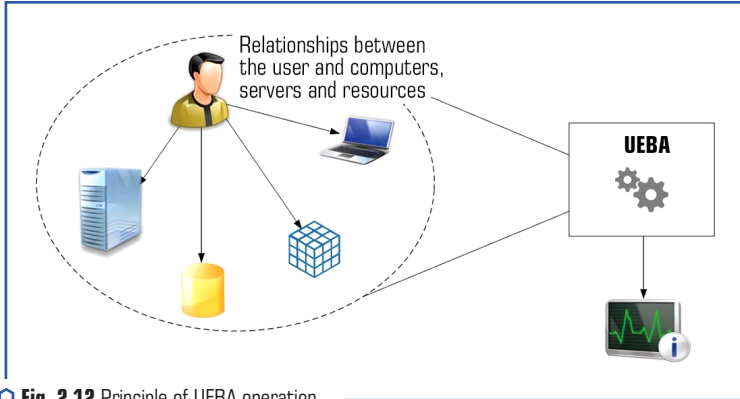


Fig. 2.12 Principle of UEBA operation

Without a system that can look at all the data at scale and make correlations not only by traffic pattern, but also by user profile, the chances of false positives for security tools increase. For example, when there is a UEBA system within the organization, which serves as the main tool for detecting malicious activity through the analysis of the behavior of users and objects in the network. The UEBA system knows which servers' users usually access, which resources they visit, which operating system is used to access these resources, and it also knows the geographic location of users. **Fig. 2.13** shows an example of this type of detection from Microsoft's Advanced Threat Analytics (ATA), which uses behavioral analytics to detect suspicious behavior. Let's note that in this case the message is quite clear. It says that the administrator did not perform these actions last month, as a result the data does not correlate with other accounts in the organization. This warning cannot be ignored because it is contextualized, which means that it analyzes the data collected from different angles to perform a comparison and decide whether to issue an alert or not.

The UEBA system within an organization can help the security team be more proactive and gain more tangible data for accurate response. The UEBA system consists of several modules, and another module is advanced threat detection, which looks for known vulnerabilities and attack patterns. **Fig. 2.14** shows how Microsoft ATA detects a Pass-the-ticket attack.

Because there are different ways to perform this attack, advanced threat detection cannot only look for the signature, it must look for the attack pattern and what the attacker is trying to do. This is much more efficient than using a signature-based system. It also looks for suspicious behavior that comes from normal users who shouldn't be performing certain tasks. For example, if a normal user tries to run NetSess.exe in the local domain, Microsoft ATA treats this as traversal of SMB sessions, which, from the attacker's point of view, is usually done during the reconnaissance phase. For this reason, Microsoft ATA issues a warning when the user attempts to run NetSess.exe.

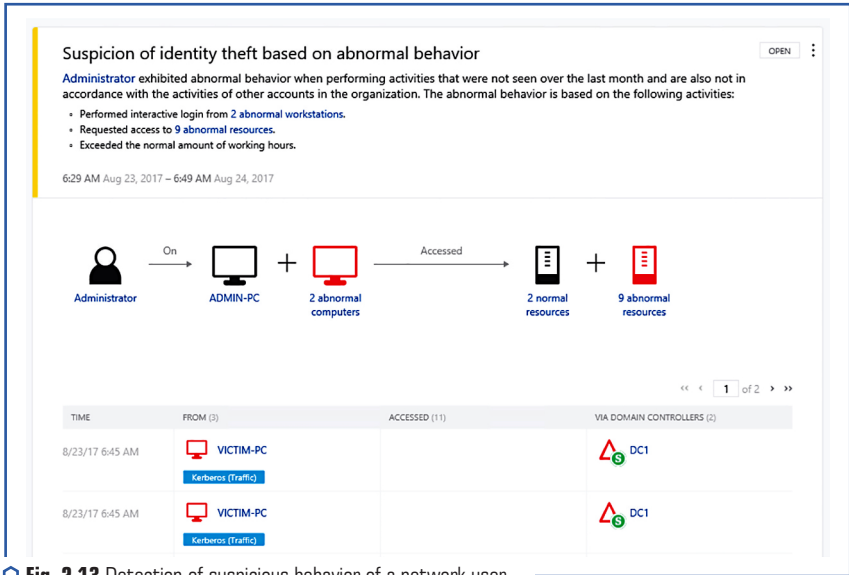


Fig. 2.13 Detection of suspicious behavior of a network user

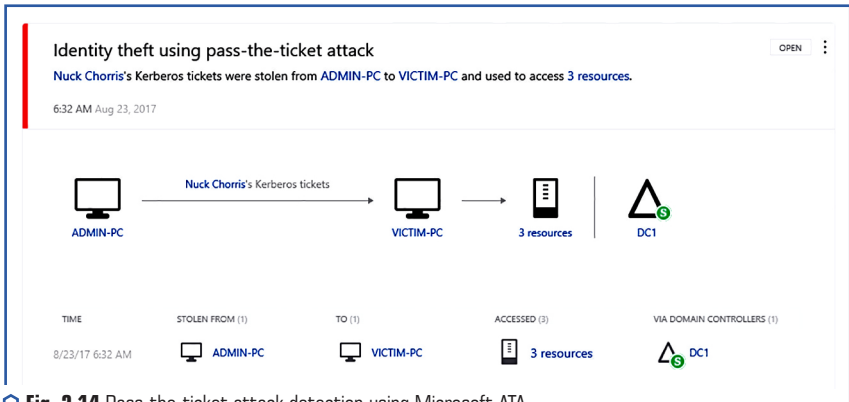


Fig. 2.14 Pass-the-ticket attack detection using Microsoft ATA

Attackers will not only exploit vulnerabilities, but also take advantage of misconfigurations in the targeted system, such as incorrect protocol implementation and lack of protection. For this reason, UEBA will also detect systems that lack a secure configuration. Fig. 2.15 shows how Microsoft ATA detects a service that provides access to account credentials because it uses the LDAP protocol without encryption.

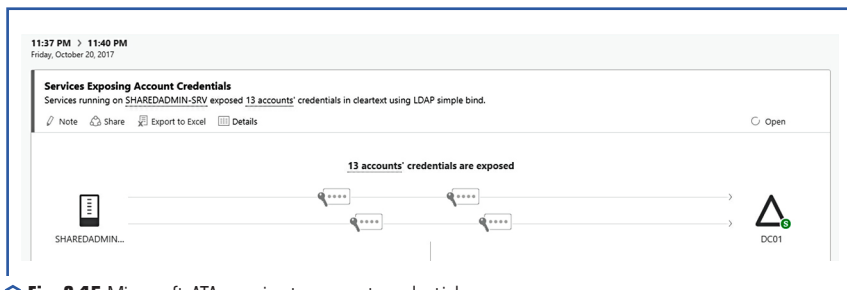


Fig. 2.15 Microsoft ATA warning to account credentials

Using the same principles previously discussed when looking at IDS, where to install UEBA will vary depending on your company's needs and vendor requirements. Microsoft ATA, which was used in the examples described in the section, requires the use of traffic mirroring with a domain controller (traffic mirroring with a domain controller). ATA will not affect network throughput as it will only listen to controller traffic.

When cybersecurity professionals need to take countermeasures to protect a hybrid environment, they should expand their understanding of the current threat landscape and perform an assessment to verify the ability to continuously connect to the cloud and assess the impact on the overall security posture. In the hybrid cloud, most companies prefer to use the IaaS model [31]. Although the adoption of this model is increasing, according to the Oracle study, the security aspect is still a major concern. According to an Oracle report, long-term users of IaaS believe that the technology will ultimately affect security. It actually has a positive impact, and this is where the cyber defense team should focus their efforts to improve the overall detection process. The goal is to use the power of the hybrid cloud to contribute to the overall security concept. The first steps are establishing a good partnership with the deployed cloud provider and understanding what security capabilities the provider offers and how those capabilities can be leveraged in a hybrid environment. This is important because some capabilities are only available in the cloud and not on-premises.

Azure Security Center

The reason for considering using Azure Security Center to monitor a hybrid environment is that the center agent can be installed on a local computer (Windows or Linux), on a virtual machine running on Azure or on AWS, which is quite relevant today. This flexibility is important, and centralized management is important for a cyber defense team. Security Center uses intelligent security tools and advanced analytics to detect threats faster and reduce the number of false positives. Ideally, using a single window system to visualize alerts and suspicious activity across all workloads, the basic topology looks similar to that shown in **Fig. 2.16**.

When Security Center is installed on work computers, it will collect ETW (Event Tracing for Windows), operating system log events, running processes, computer name, IP addresses, and registered users. These events go to Azure and are stored in the personal workspace storage.

Security Center will analyze this data using methods such as:

- cyber intelligence;
- behavioral analytics;
- detection of anomalies.

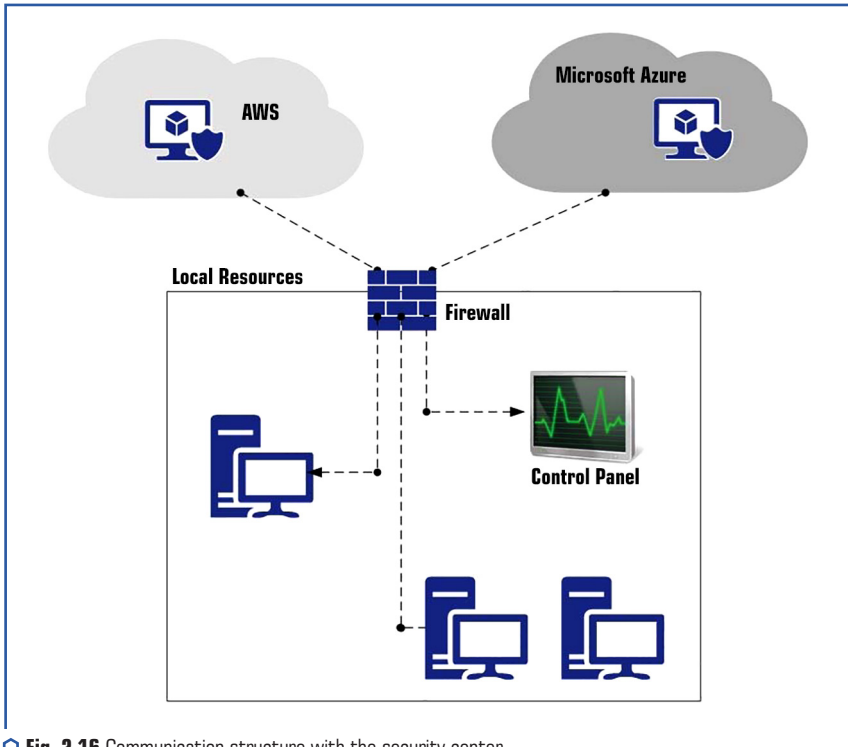


Fig. 2.16 Communication structure with the security center

After evaluating this data, the security center will trigger an alert based on the priority and add it to the monitoring dashboard as shown in the Fig. 2.17.

Let's note that the first alert has a different icon and is called Security Incident Detected. This is because it has been identified, and two or more attacks are part of the same command and control server (the attackers' C&C server) directed against a certain resource. This means that, when the security center collects data in order to find the relationship between events, it does this automatically and provides relevant alerts for analysis. When to click on this notification, the following window will appear (Fig. 2.18).



Fig. 2.17 Microsoft Azure Security Center Notification Panel

In the lower part of this page in **Fig. 2.18** shows all three attacks (in order of occurrence) on the attacked resource VM1 and the severity level assigned by the Microsoft Azure Security Center. Here is one important observation regarding the benefits of using behavioral analytics for threat detection. This is the third notification (**Fig. 2.18**) Multiple Domain Accounts Queried. The command that was executed to issue this alert is: `netuser<username> /domain`. However, to decide that this looks suspicious, it is necessary to look at the normal behavior of the user who executed the command and compare that information with other data that, when analyzed in context, would be categorized as suspicious.

As it is possible to see from this example, hackers use built-in system tools and a "native" command-line interface to carry out their attack. For this reason, it is extremely important to have a command line call logging tool available.

The security center will also use statistical profiling to build traditional baselines and anomaly alerts that match the potential attack vector. This is useful in many scenarios. A typical example is a deviation from normal activity. For example, suppose a host initiates an RDP connection 3 times a day, but on a given day hundreds of attempts are made. When such a deviation occurs, an alert should be issued to warn of it.

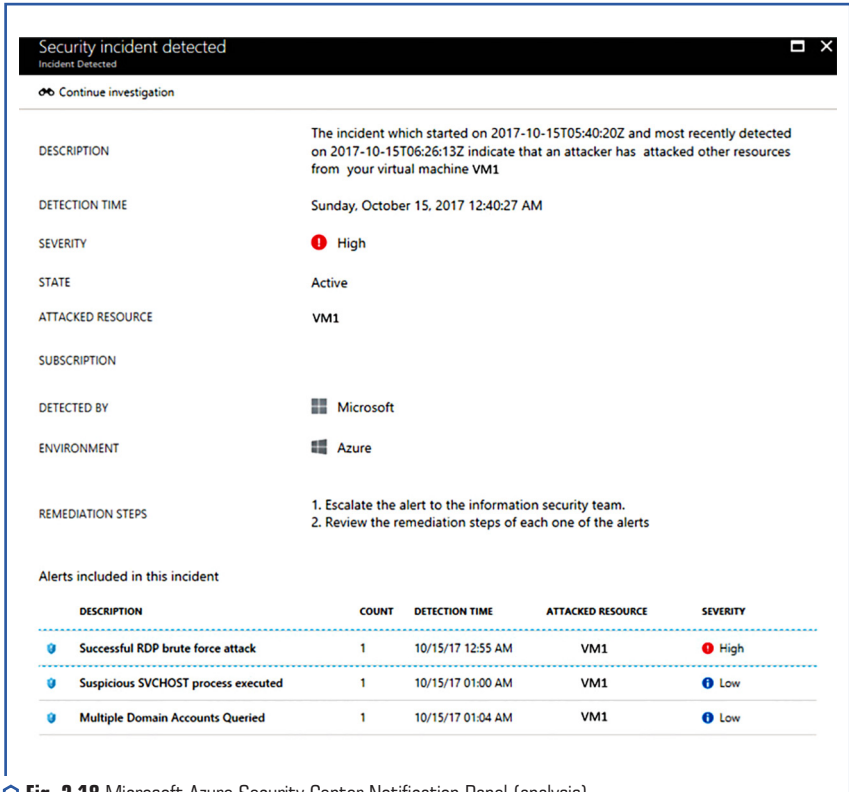
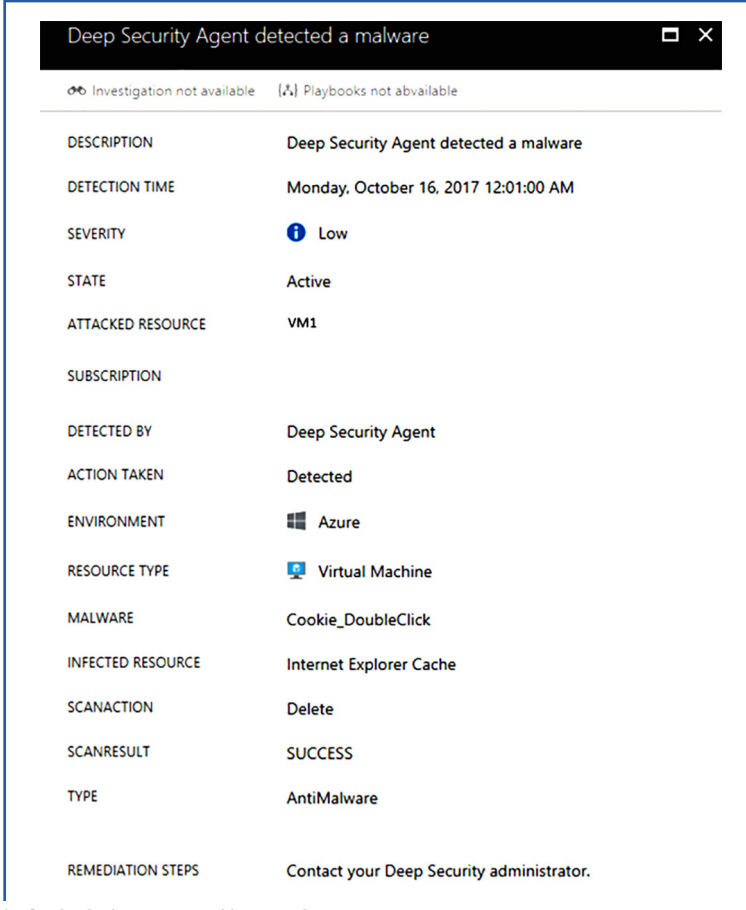


Fig. 2.18 Microsoft Azure Security Center Notification Panel (analysis)

Another important aspect of working with a cloud service is built-in integration with other providers. Security Center can integrate with many other solutions such as Barracuda, F5, Imperva and Fortinet for Web Application Firewall, among others for endpoint protection, vulnerability assessment and next generation firewall. The image below shows an example of such integration (**Fig. 2.19**).

Let's note that this alert was generated by the Deep Security Agent, and since it is integrated with Security Center, it will appear on the same dashboard as other events detected by Security Center.

It should be remembered that the security center is not the only solution that will monitor systems and integrate with other security system providers. There are many Security Information and Event Management (SIEM) solutions for information security and event management, such as Splunk and LogRhythm, that will perform a similar type of monitoring.



The screenshot shows a window titled "Deep Security Agent detected a malware". At the top, there are two status indicators: "Investigation not available" and "Playbooks not available". Below this is a table of alert details.

DESCRIPTION	Deep Security Agent detected a malware
DETECTION TIME	Monday, October 16, 2017 12:01:00 AM
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	VM1
SUBSCRIPTION	
DETECTED BY	Deep Security Agent
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
MALWARE	Cookie_DoubleClick
INFECTED RESOURCE	Internet Explorer Cache
SCANACTION	Delete
SCANRESULT	SUCCESS
TYPE	AntiMalware
REMIEDIATION STEPS	Contact your Deep Security administrator.

Fig. 2.19 Alert generated by Deep Security Agent

CONCLUSIONS

The principles of information security management according to the international standard ISO/IEC 27001 state that an organization must develop, implement and maintain a coherent set of policies, processes and systems to manage risks and threats to its information assets, thus ensuring acceptable levels of information security risk. According to this standard, it is necessary to develop an effective security policy for each enterprise depending on many factors (field of activity,

network configuration, software, etc.).

Although cybercrime is quite an actual problem, protecting information in terms of confidentiality, availability and integrity is not as easy as it might seem at first glance. It is important to constantly use new methods of protection, because criminals are constantly working and looking for new ways. That is why this section discusses modern and effective cyber protection tools for business entities. Methods and algorithms of security systems against unauthorized intrusions are usually developed for a specific object of protection. But regardless of the object of protection, it will be a large commercial network, a state-level server or a mobile device of a simple user, there is one common goal, which is to protect data as the main element of information security. To protect any system, it is necessary to first detect an intrusion (attack), regardless of the type, it will be viruses (classic file viruses or Ransomware), phishing, DDoS attacks, botnets, backdoors or other hacking attempts, this is the task of intrusion detection systems. The next stage is to decide how to eliminate this cyber-attack and, based on this experience, to create a reliable protection algorithm against threats of this type, this is the task of intrusion prevention systems. There are different operating practices of intrusion detection and prevention systems, but, as a rule, the algorithm is the same, when detecting and eliminating attacks, the task of security systems is also to create patterns of potential threats. In the further process of continuous monitoring and data scanning, data is constantly compared with templates of user and service information, as well as with templates and indicators of threats based on previous experience, not only one's own, within the local network or system, but also on a global scale [18]. That is, detection and prevention of network attacks is one of the most important tasks of the company's network cyber security policy. That is why this article considered various types of intrusion detection mechanisms and indicated the advantages of their use. Intrusion prevention systems that work on the basis of rules and anomalies are also analyzed in detail. Currently, there are various cyber protection systems (Acunetix, Azure Security Center, Invicti (formerly Netsparker), ManageEngine Vulnerability Manager Plus, System Mechanic Ultimate Defense, Microsoft Advanced Threat Analytics, SecPod SanerNow, Solar Winds Security Event Manager) with a template database of all threats, which were discovered earlier in the world. There are also many sites where it is possible to get information about new indicators and patterns, as well as contribute to the cyber security IT community by sharing your attack types if they are not available on this platform. It is very important that cyber-attack protection systems compare all data on a wide scale and make correlations not only by the traffic pattern, but also by the user profile, because otherwise the chances of false positives increase [18].

In this section, Microsoft ATA and Azure Security Center were used as an example, which was used as a hybrid solution for behavioral analysis of computer network users. Based on the considered concept of detection and prevention of intrusions, it is possible to build an effective notification system for network protection, which is the basis of a cyber security strategy according to international standards.

Therefore, creating an effective cyber security policy and managing it is a rather complex process that requires a combination of various tools, methods and specialists. First, identify resources

and assess risks, then create processes to address cybersecurity threats. Develop a plan to help the cybersecurity team respond to security breaches. Track your goals and assess your security level with the specialized solution outlined in this section.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Ukraina 2030E – kraina z rozvinutoyu cifrovoyu ekonomikoyu. Available at: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>
2. Onyshchenko, S., Skryl, V., Hlushko, A., Maslii, O.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Inclusive Development Index. Proceedings of the 4th International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 779–790. doi: https://doi.org/10.1007/978-3-031-17385-1_66
3. European Commission. International Digital Economy and Society Index 2022 – Executive Summary. Available at: <https://nqa.gov.ua/news/index-cifrovoi-ekonomiki-2022-zvit-evropejskoi-komisii/>
4. European Commission. Digital Economy and Society Index (DESI) 2022. Available at: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>
5. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. *International Journal of Engineering & Technology*, 7 (3.2), 447–452. doi: <https://doi.org/10.14419/ijet.v7i3.2.14569>
6. Glushko, A. D. (2013). Directions of Efficiency of State Regulatory Policy in Ukraine. *World Applied Sciences Journal*. Pakistan: International Digital Organization for Scientific Information, 27 (4), 448–453.
7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku "Pro Stratehiu informatsiinoi bezpeky". Ukaz Prezydenta Ukrainy No. 685/2021. 28.12.2021. Available at: <https://zakon.rada.gov.ua/laws/show/en/685/2021#Text>
8. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiu kiberbezpeky Ukrainy". Ukaz Prezydenta Ukrainy No. 447/2021. 26.08.2021. Available at: <https://www.president.gov.ua/documents/4472021-40013>
9. Saxena, H., Mittal, A. (2022). Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022. Available at: <https://www.cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022>

10. Onyshchenko, S., Hlushko, A. (2022). Analytical dimension of cybersecurity of Ukraine in the conditions of growing challenges and threats. *Economics and Region*, 1 (84), 13–20. doi: [https://doi.org/10.26906/EiR.2022.1\(84\).2540](https://doi.org/10.26906/EiR.2022.1(84).2540)
11. Onyshchenko, V., Onyshchenko, S., Maslii, O., Maksymenko, A.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic. Proceedings of the 4th International Conference on Building Innovations. *Lecture Notes in Civil Engineering Vol. 299*. Cham: Springer, 749–760. doi: https://doi.org/10.1007/978-3-031-17385-1_63
12. Borenkov, A. (2023). TOP 10 Cybersecurity Threats to Businesses in 2023. Available at: <https://www.bdo.ua/en-gb/insights-1/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023>
13. Onyshchenko, S., Bilko, S., Yanko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Business Information Security Proceedings of the 4th International Conference on Building Innovations. *Lecture Notes in Civil Engineering Vol. 299*. Cham: Springer, 769–778. doi: https://doi.org/10.1007/978-3-031-17385-1_65
14. Nayak, Mr. P., Sufiyan, M., Monisha, N. S., Bhaskar, M. G., Raju, M. (2022). Review Paper on Cyber Security and Types of Cyber Attacks. *International Journal of Advanced Research in Science, Communication and Technology*, 2 (1), 732–735. doi: <https://doi.org/10.48175/IJARSC-7043>
15. Fedor, O. (2022). 93 Must-Know Ransomware Statistics. Available at: <https://www.antivirusguide.com/cybersecurity/ransomware-statistics/>
16. Glushko, A., Marchyshynets, O. (2018). Institutional Provision of the State Regulatory Policy in Ukraine. *Journal of Advanced Research in Law and Economics*, 9 (3), 941–948. doi: [https://doi.org/10.14505/jarle.v9i3\(33\).18](https://doi.org/10.14505/jarle.v9i3(33).18)
17. Za pershyi misiats roboty systemy Protective DNS na ponad 30% zmenshylys vtraty ukrainstiv vid finansovoho fishynhu. Available at: <https://inshe.tv/suspilstvo/2023-03-16/747356/>
18. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. *Lecture Notes in Civil Engineering Vol. 299*. Cham: Springer, 791–803. doi: https://doi.org/10.1007/978-3-031-17385-1_67
19. Zhao, J., Yue, X., Feng, C., Zhang, J., Li, Y., Wang N. et. al (2022). Survey of Data Privacy Security Based on General Data Protection Regulation. *Journal of Computer Research and Development*, 59 (10), 2130–2163. doi: <https://doi.org/10.7544/issn1000-1239.20220800>
20. Schütze, B.; Hübner, U. H., Wilson, G. M., Morawski, T. S., Ball, M. J. (Eds.) (2022). Data Protection and Data Security in the EU: the European General Data Protection Regulation. *Nursing Informatics*. Cham: Springer, 437–451. doi: https://doi.org/10.1007/978-3-030-91237-6_29
21. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, 12 (6), 1333. doi: <https://doi.org/10.3390/electronics12061333>

22. Onyshchenko, S., Hlushko, A., Maslii, O., Skryl, V.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2022). Risks and Threats to Economic Security of Enterprises in the Construction Industry Under Pandemic Conditions. Proceedings of the 3rd International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 181. Cham: Springer, 711–724. doi: https://doi.org/10.1007/978-3-030-85043-2_66
23. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2022). Increasing Information Protection in the Information Security Management System of the Enterprise. Proceedings of the 3rd International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 181. Cham: Springer, 725–738. doi: https://doi.org/10.1007/978-3-030-85043-2_67
24. Makarenko, O., Yanko, A. (2022). Concept of the system of detection and prevention of networks. *Control, Navigation and Communication Systems*, 2 (68), 59–67. doi: <https://doi.org/10.26906/SUNZ.2022.2>
25. Diogenes, Y., Ozkaya, E. (2019). *Cybersecurity Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals*. Packt Publishing Ltd.
26. Othman, S. M., Alsohybe, N. T., Ba-Alwi, F. M., Zahary, A. T. (2018). Survey on Intrusion Detection System Types. *International Journal of Cyber-Security and Digital Forensics*, 7 (4), 444–462. doi: <http://dx.doi.org/10.17781/P002525>
27. Northcutt, S., Novak, J. (2002). *Network Intrusion Detection: An Analyst's Handbook*. Indianapolis: New Riders Publishing, 478.
28. Kalaivani, A., Pugazendi, R. (2023). A Review on Intrusion Detection System and its Techniques. *Data Analytics and Artificial Intelligence*, 3 (2), 132–137. doi: <https://doi.org/10.46632/daai/3/2/24>
29. Li, J. (2022). Network Intrusion Detection Algorithm and Simulation of Complex System in Internet Environment. 2022 4th International Conference on Inventive Research in Computing Applications, Coimbatore: IEEE, 520–523. doi: <https://doi.org/10.1109/ICIRCA54612.2022.9985720>
30. Collins, M. (2017). *Network Security Through Data Analysis: From Data to Action*. O'Reilly Media, Inc.
31. Chowdhury, P., Paul, S., Rudra, R., Ghosh, R.; Joshi, A., Mahmud, M., Ragel, R.G. (Eds.) (2023). Cyber-Attack in ICT Cloud Computing System. *Information and Communication Technology for Competitive Strategies. Lecture Notes in Networks and Systems Vol. 400*. Singapore: Springer, 115–121. doi: https://doi.org/10.1007/978-981-19-0095-2_12

CHAPTER 3

STRENGTHENING THE SECURITY OF UKRAINIAN STRATEGICALLY IMPORTANT ENTERPRISES AS A BASIS FOR THE NATIONAL ECONOMY SUPPORTING AND RESTORING**ABSTRACT**

The study is devoted to solving the problem of strengthening the security of strategically important enterprises in Ukraine by developing effective forms of implementing the state regulatory policy in this direction. The issues of identification of strategically important enterprises and the formation of their security at the state level as a basis for supporting and restoring the national economy have been updated. The study assessed the level of Ukrainian economic security, which confirmed the need to strengthen it, primarily through the revitalization of business entities. Deregulation of entrepreneurial activity is the basis for the efficient and stable functioning of Ukrainian businesses. In this aspect, considering the key provisions of the Draft Plan for the Recovery of Ukraine, the strategic directions for the deregulation of business activities in Ukraine, including strategically important enterprises, have been determined. One of them is the state regulatory policy institutional support regulatory policy improvement.

The analysis of the existing institutional support of the state regulatory policy in relation to strategically important enterprises has been carried out. The basis for the formation of effective forms of the state regulatory policy implementation of support and strengthening the security of strategically important enterprises is the need to improve the current legislation, the formation of effective institutional and organizational support and the clustering of national economy on the basis of strategically important enterprises with the possibility of creating integrated corporate structures.

The study proposes a model for the process of assessing the effectiveness of the implementation of the state regulatory policy to ensure the security of strategically important enterprises, which provides the regulatory authorities with a tool to influence its level ensuring economic development and social stability in Ukraine in the future.

KEYWORDS

Strategically important enterprises, security, economic security, state regulatory policy, business environment, martial law, financial support, institutional support.

The national economy of Ukraine has been functioning for the last year in the conditions of unprecedented challenges and threats caused by the military aggression of the Russian Federation. The support and restoration of the economic system depend on the efficiency of the economic entities activities, primarily those that are critically important in terms of ensuring national economy security. The status of such economic entities can be legitimately defined as strategically important. In the Ukrainian institutional environment, the concept of "strategic importance enterprising for the state economy and security" has been used with the aim of ensuring the implementation of national interests in the sphere of state property privatization and reducing possible threats to the state economic security. In the conditions of war, the problem of identifying strategically important enterprises and forming their security at the state level acquires special relevance and requires the development of effective forms of state regulatory policy implementation of in this direction.

3.1 ASSESSMENT OF THE UKRAINIAN ECONOMIC SECURITY LEVEL

The military aggression of the Russian Federation, which entailed a number of unprecedented threats, has actualized the issues of Ukrainian economic security strengthening as the basis for the stability of both country's functioning and ensuring national security generally. The study is based on the application of both comparative analysis principles and the indicator method in assessing the economic security level. To summarize the data on the sample, descriptive statistics methods have been used applying such statistical indices as the mean value and standard deviation, which enabled to assess the impact of sub-indices on the Ukrainian economic security level.

According to the Guidelines for calculating the Ukrainian economic security level [1], the components of economic security are: production, demographic, energy, foreign economic, investment and innovation, macroeconomic, food, social, and financial security.

The production security indicator characterizes the state and development of the production sector. Its level determines the efficiency of the use of the country's production capacities, the possibilities of modernization and expanded reproduction, the innovativeness of production and the competitiveness of the national economy.

Demographic security is defined as the state of protection of the country and society from demographic threats. A sufficient level of demographic security ensures the development of Ukraine on the basis of balancing the demographic interests of the state and society in accordance with the constitutional rights of Ukrainian.

The energy security indicator is a state of the economy that ensures efficient use of energy resources, a sufficient number of energy producers and suppliers in the energy market, and availability, differentiation and environmental friendliness of energy resources.

Foreign economic security implies coherence between foreign economic activity and national economic interests. Its sufficiency is characterized by minimizing the state's losses from negative external economic factors and the possibility of creating the necessary conditions for economic development.

The investment and innovation security indicator allows to characterize the state of the economic environment in a country. It shows the level of development of high-tech production, integration of research and production, and deepening of the national economy's specialization in the production of high value-added products.

Macroeconomic security characterizes the achievement of a balance in macroeconomic reproduction proportions.

The food security indicator shows the ability of production to meet the needs of society for food of appropriate quality, provided that it is balanced and affordable.

Social security characterizes the ability of a country to ensure a high standard of living for its population.

The financial security indicator reflects the state of the country's financial system, the ability to create financial conditions for stable social and economic development, the ability to ensure its resilience to financial shocks and imbalances, and to create conditions for achieving the integrity and unity of the country's financial system.

The structural components of financial security are as follows: banking security, non-banking financial sector security, debt security, budget security, currency security, and monetary security.

Banking security characterizes the level of financial strength and stability of the country's banking institutions, which, in turn, makes it possible to ensure a high level of efficiency of the country's banking system. The security of the non-banking financial sector determines the level of development of the insurance and stock markets, and the satisfaction of society's needs for financial instruments and services. Debt security characterizes the level of the country's domestic and foreign debt, the efficiency of using domestic and foreign loans, and the optimal ratio of these loans. The budgetary component of financial security is determined by the ability to ensure financial stability and solvency of public finances. The level of public confidence in the national currency and its stability determine currency security. Monetary security is a state of the monetary system that allows providing national economic entities with high-quality and affordable credit resources in amounts and on terms favorable for achieving economic growth of the national economy.

In order to substantiate the priority areas for restoring Ukraine's economic development and security, and to identify priority measures to support financial stability and restore critical infrastructure, it is necessary to analyze the level of economic security by certain sub-indices. Such an approach will allow to identify the level of each component of economic security and outline the strategy of the state regulatory policy.

Based on the Guidelines for calculating the Ukrainian economic security level and official data from Ministry of Economy of Ukraine, the absolute values of indicators of the economic security components have been calculated and integral indicators have been determined, summarized in the **Table 3.1**.

Based on the estimation of the average levels of the components of the economic security integral indicator, it is legitimate to note that the following components are in the unsatisfactory zone: production, demographic, energy, financial and social (within 40–59 %); in the danger zone (20–39 %) foreign economic, macroeconomic and investment and innovation. The most

unstable situation during the period under study has been observed in the dynamics of energy security (standard deviation 5.87) and macroeconomic security (standard deviation 4.91). The most stable indicators for 2013–2020 are investment and innovation (1.77) and social security (2.26).

● **Table 3.1** Integral indicators of the Ukrainian economic security components for 2013–2020 years

Indicator	2013	2014	2015	2016	2017	2018	2019	2020	max	min	Average value	Standard deviation
Integral indicator of production security, %	49	51	47	58	59	58	57	54	59	47	54.13	4.61
Integral indicator of demographic security, %	46	45	43	46	40	41	39	40	46	39	42.50	2.88
Integral indicator of energy security, %	39	47	45	58	54	53	49	49	58	39	49.25	5.87
Integral indicator of foreign economic security, %	29	32	33	35	36	36	40	44	44	29	35.63	4.69
Integral indicator of investment and innovation security, %	35	30	33	30	30	31	31	31	35	30	31.38	1.77
Integral indicator of macroeconomic security, %	39	33	30	38	37	40	45	43	45	30	38.13	4.91
Integral indicator of food security, %	86	94	92	92	91	90	89	85	94	85	89.88	3.09
Integral indicator of social security, %	62	57	55	56	59	59	60	59	62	55	58.38	2.26
Integral indicator of financial security, %	50	40	35	38	40	45	42	40	50	35	41.25	4.56
Integral indicator of economic security, %	47	45	44	48	48	49	49	48	49	44	47.25	1.83

Note: compiled by the author according to [1, 2]

The presence of the noted problematic aspects in the Ukrainian economic security confirms the level of the integral indicator (**Fig. 3.1**).

With the maximum value of the country's integral indicator level of economic security at 100 %, the largest was observed in 2018–2019. The drop in the level of economic security in 2015 is associated with the military aggression of the Russian Federation in the east of the country, and in 2020 with the COVID-19 pandemic and the quarantine restrictions caused by it [3].

The optimal zone for the level of economic security is an indicator of more than 80 % (80–100 %), satisfactory 60–79 %, unsatisfactory 40–59 %, dangerous – the range of 20–39 %, critical – less than 20 % (0–19 %). For the entire analyzed period 2013–2020, the level of economic

security was at an unsatisfactory level (40–59 %), but did not go beyond the safe zone. At the same time, the predicted negative dynamics of the integral indicator, described by a polynomial trend line, confirms the current realities in connection with the war in Ukraine.

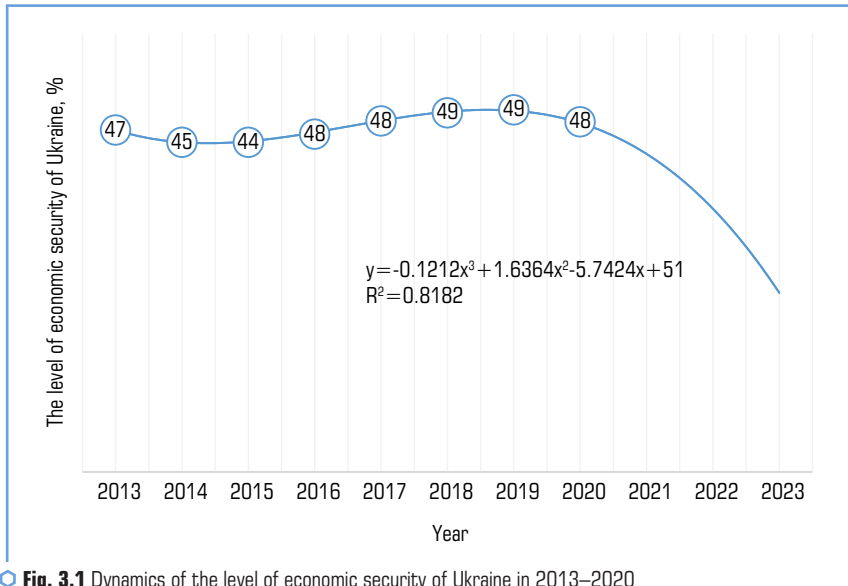


Fig. 3.1 Dynamics of the level of economic security of Ukraine in 2013–2020
 Note: compiled by the author

In order to strengthen economic security, public authorities should actively implement regulatory measures in the following areas.

1. Support domestic market. In order to stabilize and restore the national economy, it is necessary to further reduce the regulatory and administrative burden on business, in particular through the introduction of deregulation measures based on a risk-based approach to develop business self-regulation; introduce new and expand existing support tools for small and medium-sized businesses, including financial ones [4]. It is legitimate to define the food and light industry, the IT sector as a priority for the resuscitation of the domestic market. Regulatory support needs a machine-building complex. Total defense spending in 2023 exceeds 1 trillion UAH. Thus, at least a partial renewal of the capacities of the military-industrial complex through the use of enterprises of the machine-building complex can become a significant factor in the industrial production growth [5].

2. Support for monetary stability. It is worth noting that since the beginning of the full-scale invasion of the Russian Federation, a number of financial support instruments have been used. In April 2023, the Financial Stability Board created a working group for the development of the domestic debt market with the participation of representatives of the National Bank of Ukraine and

the Ministry of Finance of Ukraine. The working group was established as part of the implementation of the Memorandum on Economic and Financial Policy with the International Monetary Fund, according to which Ukraine undertook to avoid emission financing of the state budget and develop the domestic debt market by expanding and diversifying the circle of investors in government securities, including through the return of non-residents to domestic bond market. In addition, since May 2023, the procedure for assessing the stability of the banking system in wartime conditions has begun. Also, in order to strengthen market incentives for banks to attract fixed-term deposits of the population in the national currency, reduce risks for the foreign exchange market, the operational design of monetary policy has been updated, providing for a reduction in the rate on deposit certificates and the introduction of new limited three-month deposit certificates at a fixed rate at the accounting level [6]. These changes help protect citizens' savings from inflationary depreciation, reduce price pressures, and promote a culture of time savings in the hryvnia.

3. Restoration of balance in foreign and domestic trade. Military aggression has led to an increase in the disproportion between the internal and external trade markets. Limiting the process of currency laundering from the Ukrainian market should be an element of restoring economic security.

4. Restoration of infrastructure. The main task should be considered the restoration of the energy infrastructure, constantly suffering as a result of targeted enemy attacks. At the same time, it is reasonable to consider as shifts the adaptation of both businesses and households to the risks of deep blackouts, the improvement of the technology for protecting and restoring energy facilities.

Consequently, modern threats to the Ukrainian economic security are both modern military and structural by nature. Attacks on infrastructure facilities, the occupation of some parts of Ukrainian territory, the budget crisis and other challenges have exacerbated problems in the functioning of the national economy. In order to restore Ukrainian economic development and security, it is necessary to support the domestic market, take measures to further support financial stability and restore critical infrastructure.

3.2 ANALYSIS OF BOTH BUSINESS ENVIRONMENT AND STATE REGULATORY POLICY IN THE ASPECT OF STRENGTHENING ECONOMIC SECURITY UNDER MARTIAL LAW

The experience of the world's leading countries shows that a favorable business environment is one of the main factors of economic growth. In this regard, the state regulatory policy should be aimed at improving the regulatory environment, including through deregulation. Deregulation implies the abolition of regulatory restrictions and inefficient control procedures, excessive licensing, outdated certification, monitoring and other restrictions on business activities.

Regulatory reform in Ukraine aimed at improving the business environment began in 1997 with the creation of a special institution for the development and implementation of regulatory policy in the field of entrepreneurship – the State Committee of Ukraine for Entrepreneurship Development. Since then, the State Committee for Entrepreneurship Development has suspended

about 90 regulatory acts that hindered business activity. The legislative basis for the formation of a favorable regulatory environment was laid down by the Decrees of the President of Ukraine "On Elimination of Restrictions Hindering the Development of Entrepreneurial Activity" of February 03, 1998 and "On Some Measures for Deregulation of Entrepreneurial Activity" of July 23, 1998. These Decrees identified deregulation as one of the priority areas of reforming economy's state regulation and outlined a number of priority measures to improve the business environment. In 1998 and 1999, as part of implementation of the provisions of these decrees, the State Committee for Entrepreneurship Development reviewed, approved, and commented on more than 300 draft regulatory documents. In some cases, the economic benefits of deregulation amounted to tens of millions hryvnia saved by entrepreneurs, consumers and the public sector. In general, the conditional economic effect of the Committee's actions to deregulate business activities, according to international experts (USAID), amounted to about \$ 450 million [7].

Despite the positive results from the abolition of regulations that hindered the development of entrepreneurship, these measures were not enough to bring about qualitative changes in the business environment. There was a need to create a mechanism for effective influence on economic and social processes, to introduce such principles of state regulatory policy that would ensure that the process of creating a new regulatory act would best meet the needs of society.

In 2000, the President of Ukraine adopted the Decree of the President of Ukraine "On the Introduction of a Unified State Regulatory Policy in the Field of Entrepreneurship", which laid down the foundations and procedure for the implementation of state regulatory policy in the field of entrepreneurship. In particular, it defined the procedure for adopting regulatory acts, which was aimed at improving their quality and efficiency and reduced the costs of business entities and the state. At the same time, by adopting the Law of Ukraine "On Licensing of Certain Types of Economic Activity", a new model of state regulation of the licensing sphere is being formed as an integral part of the deregulation process.

The noted positive changes in the regulation of the regulatory framework for entrepreneurship in 1997–2000 became the basis for the legislative consolidation of the principles of state regulatory policy and the extension of their effect to the entire sphere of economic activity. In 2003, the Law of Ukraine "On the Principles of State Regulatory Policy in the Sphere of Economic Activity" was adopted, the norms of which met international standards, and their implementation allowed to reduce state interference in the activities of business entities and partially eliminate obstacles to the development of economic activity in Ukraine by introducing mandatory assessment of the economic efficiency of regulatory acts.

In recent years, the state regulatory policy has been aimed at improving and simplifying the legal regulation of economic relations, reducing the interference of state bodies in the activities of business entities. The full-scale invasion of the Russian Federation has become an unprecedented threat to the functioning of the business environment in Ukraine. This is confirmed by official data from the Center for Innovation Development, the Office for Entrepreneurship and Export Development, and the national project Diia.Business, according to which in 2022 there was the lowest dynamics of opening new business entities over the past three years (**Fig. 3.2**).

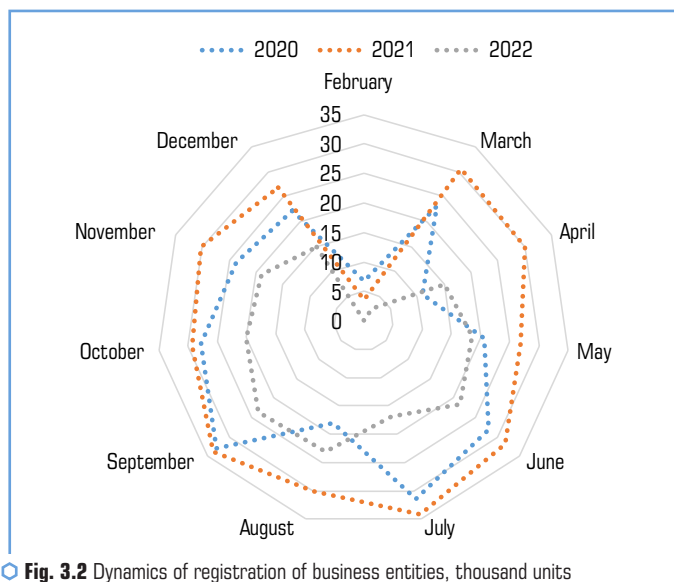


Fig. 3.2 Dynamics of registration of business entities, thousand units
 Note: compiled by the author according to [8]

The level of country's economic security directly depends on the activity of economic entities. The military anger of the Russian Federation led to the closure, temporary cessation of the functioning of many companies, inflicted large financial losses on them due to the destruction of production facilities, infrastructure, and the suspension of investment projects. Support, stabilization and recovery of the national economy in times of war depend on the ability of economic entities to adapt to changes in the external environment, in particular, the promptness of decision-making in terms of maintaining production capacities, jobs, readiness for relocation and the level of state regulatory policy effectiveness.

It should be noted that in the first six months of the war, more than 78 thousand business entities closed, 419 went bankrupt. Since the beginning of the full-scale invasion of the Russian Federation, only in July, the number of newly created entities exceeded the number (Fig. 3.3).

It should be noted that the total amount of direct damage caused by the aggressor state during the year of the war to individuals – entrepreneurs and legal entities is estimated by experts at \$ 13 billion, of which \$ 9 billion is damage caused to large and medium-sized businesses [2].

The need to preserve entrepreneurial potential and form the foundation for the return of business, forced to suspend operations, required the introduction of operational regulatory tools to support business entities. At the same time, the effectiveness of the implemented regulatory instruments was determined by the optimal combination of the levers of the state regulatory policy: legal, administrative and economic. The ability to discuss the presence of legal levers in the struc-

3 STRENGTHENING THE SECURITY OF UKRAINIAN STRATEGICALLY IMPORTANT ENTERPRISES AS A BASIS FOR THE NATIONAL ECONOMY SUPPORTING AND RESTORING

ture of regulatory policy enables it to be possible for certain legal acts to belong to regulatory ones. At the same time, the concept of state regulatory policy, given in the Law of Ukraine "On the Fundamentals of State Regulatory Policy in the Sphere of Economic Activity", provides for the presence of administrative and economic levers, the distinction between which is conditional. After all, in order to use the economic regulator, public authorities must first make an administrative decision. Any administrative regulator, encouraging enterprises to carry out certain actions, at the same time indirectly affects individual economic processes [9].

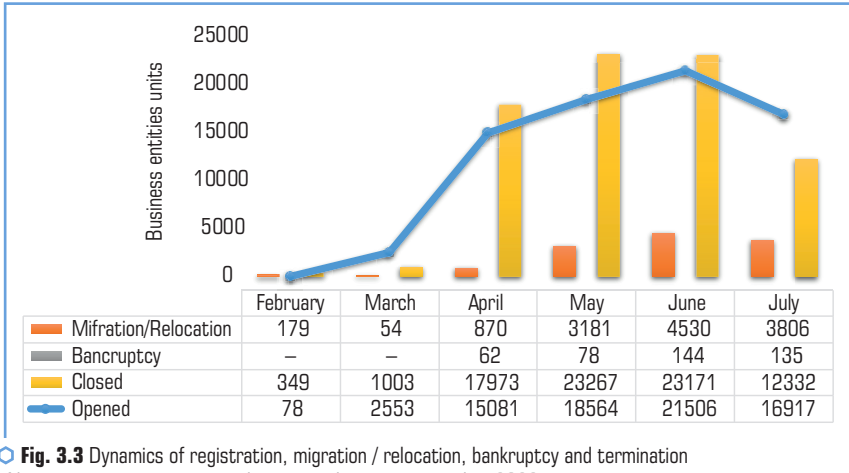


Fig. 3.3 Dynamics of registration, migration / relocation, bankruptcy and termination of business entities activity in Ukraine in February – December 2022
Note: compiled by the author according to [8]

Implemented during March-December 2022, regulatory tools for resuming business activity as part of the wartime state regulatory policy implementation included:

- business relocation program implementation to safe territories;
- financial support for business by unifying approaches, expanding goals and the circle of participants for the state programs "Affordable loans 5–7–9 %" and "Affordable financial leasing 5–7–9 %" implementation, as well as the provision of loan guarantees on a portfolio basis; grant programs implementation for starting a new business, developing entrepreneurship and training (micro-grants for creating your own business, grants for the development of a processing enterprise, state funding for planting a garden, greenhouse development funds, a grant for the implementation of a start-up, including IT sphere, funds for training IT specialties);
- formation of a state order for products in order to support the production activity of business entities;
- amendments to the tax legislation in the direction of reducing the fiscal burden on business entities;

– implementation of a number of bills to deregulate the business environment, which included, in particular, the digitalization of public services and the deregulation of the contractual labor relations regime for small and medium-sized businesses [10].

These regulatory tools have enabled to intensify the business work, to minimize obstacles to its development. According to the latest data from the Ministry of Economy, since the beginning of the relocation program, 761 enterprises have moved to safe regions, of which 588 are successfully operating in new places, 274 are in the process of searching for a suitable location or method of transportation [11]. Since the launch of the program "Affordable loans 5–7–9 %", as of December 2022, 17,359 loan agreements have been concluded for a total of UAH 72.24 billion (including 13,089 loan agreements for a total of UAH 38.39 billion by public sector banks) [12]. Since the beginning of the government program "Own business" implementation, projects of more than 3 thousand entrepreneurs have been financed for a total amount of about UAH 776.8 million. Due to the expansion of the partnership program of the Export Credit Agency by joining it with JSC CB "PrivatBank", which provides for lending to businesses for the foreign economic contracts implementation under credit expert agency insurance coverage without additional material collateral, it has enabled to simplify access to financing for business entities exporting products [13, 14].

As part of the financing program (in the amount of \$ 2 billion) for agricultural enterprises and small and medium-sized businesses, approved by the Board of Directors of the International Finance Corporation (IFC) in December 2022, it has been planned to actively attract foreign investors. A feature of the program is the permission of the IFC Corporation management, as an exception for Ukraine, to cooperate with state-owned companies. The IFC Board of Directors has approved two special projects for the private sector, both for the French company EnVivo, which has agribusiness in Ukraine; war risk insurance (through MIGA) for Raiffeisen Bank [15]. In December 2022, the Entrepreneurship Development Fund signed a loan agreement with AB "Ukrhasbank" in the amount of UAH 150 million to finance investment projects of small and medium-sized businesses in the field of energy saving as part of the project "Refinancing of energy efficient investments energy supply". During the project implementation, new approaches to lending are introduced, based on both international environmental and social standards of the Sustainable Development Finance Policy [16].

Certain financial support for entrepreneurial activity through the implementation of credit, state grant programs, programs for financing investment projects, primarily in the field of energy supply, as well as expanding partnerships for more efficient implementation of export mechanisms, has become an important factor in strengthening financial stability and an engine of business activity in high-risk conditions.

Amendments to the Tax Code enabled to introduce a new temporary mechanism for taxing business entities aimed at supporting their functioning. In particular, it is rightful to note that enterprises with an income of up to 10 billion hryvnias are given the opportunity to become payers of the single tax of the 3rd group, which provides for: a tax rate of 2 % of income (instead of 18 % of income tax); VAT (20 %) is not applied to operations on the territory of Ukraine; there is no limit

on the number of employees [17]. Changes in tax legislation, state programs implementation of financial support for business enabled to conduct business even in wartime.

The deregulation of the business environment involved a number of measures implementation to abolish requirements for obtaining licenses and permits for most types of activities, liberalizing labor relations, abolishing inspections and the absence of sanctions for late reporting, simplifying requirements for labeling food products, digitizing state services and services. Thus, by Resolution No. 314 of March 18, 2022, the Cabinet of Ministers of Ukraine introduced the declarative principle of acquiring the right to conduct economic activity without the need to obtain documents of a permissive nature, licenses, etc. Adoption of the Resolution enabled to significantly simplify the procedure for opening a business entity and became a significant step in the deregulation of economic activity, since instead of about 600 types of licenses and permits, only about 50 remained valid.

Changes to the Labor Code introduced during martial law contributed to the liberalization of labor relations. Among the main innovations: the simplified system introduction of dismissal and reduction of employees in the zone of active hostilities, the possibility of suspending the employment contract and increasing working hours from 40 to 60 hours per week, as well as reducing the number of mandatory days off to one day.

Significant relaxations have taken place in the field of tax reporting and payment of taxes, which simplifies the conduct of business activities in wartime conditions. In particular, taxpayers received the right to submit tax and other reports within 90 calendar days after the abolition of the legal regime of martial law, and therefore the responsibility for late submission of reports during martial law and 90 days after its termination also does not be applied. Also, during the period of martial law, financial sanctions do not be applied for violations related to the use of recorder of payment transactions (RRP).

It is noteworthy the significant deregulation of economic activity in the agrarian sphere. In addition to a number of legislative changes, which were aimed at supporting farmers by reducing the price of fuel and preventing its potential shortage, the Ministry of Agrarian Policy and Food of Ukraine during the martial law also canceled additional seed certification procedures, in particular, by recognizing foreign certificates, as well as the need registration of agricultural machinery. The validity of the license for the storage, transportation and use of pesticides has been extended for 90 days after its termination or cancellation.

Measures to deregulate entrepreneurial activity included the development of digitalization of public services and services. At the end of May 2022, the Ministry of Digital Transformation, together with the Ministry of Economy and BRDO (Better Regulation Delivery Office), announced the introduction of a new service for business on the Diia portal – eDeclaration. This electronic document, which execution takes no more than three minutes, enables to immediately start business and is intended to replace 374 types of permits. The Declaration service can be used by business owners whose permits have expired; individual entrepreneurs who, under martial law, have changed their place of doing business and need a license; entrepreneurs who changed the type of activity in connection with the war. The Ministry of Digital Transformation also launched beta testing of

a new service on the Diia portal – automatic registration of limited liability companies, aimed at simplifying the registration procedure for business entities and saving time for public registrars.

Important measures in the direction of deregulation and improvement of the conditions for the entrepreneurial activity implementation are the support by the Verkhovna Rada of Ukraine of draft laws No. 5371 and No. 5161. The first is aimed at deregulating the regime of contractual labor relations for small and medium-sized businesses and reducing the administrative burden on entrepreneurial activity. At the same time, contractual regulation of labor relations involves strengthening the principles of market self-regulation in terms of salaries, the workers' rights to salaries and their protection, receiving annual paid holidays and holidays without pay. Draft law No. 5161 introduces a new specific form of an employment contract with non-fixed working hours. Accordingly, the employee enables to combine both official work with several employers and have basic social guarantees.

In October 2022, the President of Ukraine signed the law "On Amendments to the Tax Code of Ukraine and Certain Other Legislative Acts of Ukraine on the Peculiarities of Taxation of Entrepreneurial Activities of Electronic Residents", which has come into force on April 1, 2023 and provides for a special status for foreigners to conduct business in Ukraine. The law is aimed at creating favorable conditions for both foreigners and stateless persons who have received e-resident status to register as an individual entrepreneur and conduct business without crossing the border. The introduction of this regulatory tool enables to create a positive investment climate, contribute to the national economy restoration and development, increase the gross domestic product and tax revenues to the state budget.

The indicated measures of deregulation of entrepreneurial activity have become the basis for the formation of a favorable regulatory environment in the context of martial law. Noting the positive changes, it is legitimate to note the need to continue deregulation. This is confirmed by the data of a study conducted in November 2022 by the Center for Innovation Development, Office for Entrepreneurship and Export Development, the national Action project and Advanter Group [18]. 16 % of surveyed business entities noted a decrease in the tax burden, 12 % – improving the conditions for doing business, 75 % – noted the need to continue the deregulation of entrepreneurial activity under martial law as a basis for supporting and restoring the national economy of Ukraine.

Since the beginning of the full-scale invasion of the aggressor on the territory of Ukraine, a number of regulatory measures have been taken to find additional sources of funding, attract international organizations to provide grants, etc. One of the main state grant programs to support business in times of war is legitimate to define the project "eРобота"/"eWork", which provides for the provision of grants for the entrepreneurship start training and development. The grant program is implemented in a number of areas, including the provision of micro-grants for starting a business ("Own business"); providing grants for the implementation of Start-up; financing of training in specialties in the field of IT; financing the development of orchards and greenhouses; grants for the processing enterprise development. In the "Own business" direction, 900 applications for a microgrant were received in four months of 2023, and 136 winners enable to receive up

to UAH 250,000 of financial support for the business projects implementation providing the creation of more than 300 new jobs. In general, in 2023, UAH 1.8 billion is allocated in the Ukrainian state budget of for 10,000 microgrants [19].

In March 2023, the Cabinet of Ministers of Ukraine announced the expansion of the list of non-refundable grants under the Work program with areas for veteran businesses [20]. Thus, veterans are able to receive up to UAH 250,000 of state funding to start their own business if one new job is created. Co-financing is also provided (70 % of state financial resources and 30 % of the entrepreneur's own funds) for both combatants' family members and combatants with experience in doing business. At the same time, the size of the grant is UAH 500,000 and 1 million, respectively.

Another state business support program, which started on February 1, 2020, is the Affordable Loans 5–7–9 % program. As part of its implementation, since the beginning and till the end of March 2023, business entities received loans from partner banks totaling UAH 185.58 billion. Since the beginning of the war launched by the Russian Federation against Ukraine, a number of changes have been made to the program related to the unification of approaches, the expansion of goals and the circle of participants, which enabled to provide financial support to a larger number of business entities. The dynamics of the level of financial support for business under the program "Affordable loans 5–7–9 %" is shown in **Fig. 3.4**.

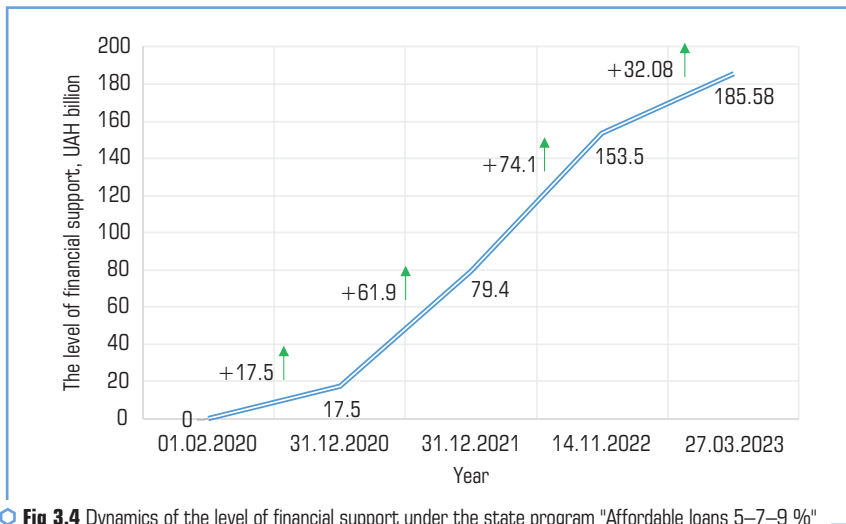


Fig 3.4 Dynamics of the level of financial support under the state program "Affordable loans 5–7–9 %"
 Note: compiled by the author according to [21]

During the war period, under the program, loan agreements were concluded in the amount of UAH 95.96 billion, of which UAH 870 million were investment loans; UAH 7.33 billion – anti-crisis loans; UAH 4.37 billion – refinancing of previously received loans, UAH 26.54 billion – loans for

agricultural producers; UAH 56.76 billion – financing of anti-war goals. In order to economically restore the affected regions, the Cabinet of Ministers of Ukraine, at the initiative of the Ministry for the Reintegration of the Temporarily Occupied Territories of Ukraine, at the beginning of April 2024 decided to allow entrepreneurs from the territories of possible hostilities and de-occupied territories to participate in the program [10, 21].

At the same time, international organizations are actively providing financial support to Ukrainian business. Thus, within the framework of the USAID program "Competitive Economy of Ukraine", grant projects "Business Continuity and Resumption" (financing the development of new products, digitalization of business processes, development of organizational potential), "Support for business participation in trade events" were launched. Grants for the implementation of business projects, investment projects, business relocation are also offered by the European Bank for Reconstruction and Development, the German government company Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), the Danish Refugee Council (DRC), the European Union under the EU4Environment program, the International Organization for Migration and the United Nations Agency for Migration (grant program under the project "Development of small and medium-sized enterprises: Economic integration of internally displaced persons and business resumption") and others.

It is important that both state and international grant programs implemented in modern conditions also aim to support innovative projects, develop the sphere of cybersecurity, healthcare, education, infrastructure, that is, they are aimed at forming the basis for the post-war recovery of the Ukrainian economy.

A certain financial support for business through the implementation of credit, grant state programs, programs for financing investment projects, as well as the expansion of international partnerships in this direction is an important factor in strengthening financial stability, a driver of business activity in conditions of high wartime risks [22] and, of course, the basis for the national economy successful recovery in the post-war period

The implementation of regulatory tools to support and develop the national economy should be systematic and consistent and based on the principles of creating a favorable regulatory environment. In order to restore the national economy, it is necessary to further reduce the regulatory and administrative burden on business by introducing deregulation measures based on a risk-based approach for the development of business self-regulation, which involves a transparent licensing system formation and partnerships development both between business entities and state regulatory authorities.

3.3 IMPROVING THE INSTITUTIONAL SUPPORT OF THE STATE REGULATORY POLICY IN TERMS OF STRENGTHENING THE STRATEGICALLY IMPORTANT ENTERPRISES SECURITY IN UKRAINE

The national economy of Ukraine has been functioning for the past year in the face of unprecedented challenges and threats caused by the military aggression of the Russian Federation.

Support and restoration of the economic system depends on the efficiency of business entities, primarily those that are critical in terms of ensuring the national economy security.

A constructive analysis of the current legislation enables to assert that there is no definition of the concept of "strategically important enterprise". There is only a list of state-owned objects of strategic importance for the state economy and security, as well as criteria for classifying business entities as having strategic importance for the state economy and security.

For the first time, a list of enterprises of strategic importance was given in the Decree of the Cabinet of Ministers of Ukraine "On approval of the list of enterprises of strategic importance for the economy and security of the state" August 21, 1997 (repealed). At the same time, the criteria for granting such status to business entities were determined six years later by the Decree of the Cabinet of Ministers of Ukraine "On determining the criteria for classifying enterprises (organizations) as having strategic importance for the economy and security of the state" dated May 15, 2003. Both the list and the criteria for classifying enterprises as strategically important were constantly changing without proper scientific justification and official explanation.

It is worth noting that the Decree of the Cabinet of Ministers of Ukraine dated January 30, 2019 approved the Procedure for the formation and maintenance of the State Register of Import Substitution and Cooperation in Strategic Industries, according to which the military-industrial complex, aviation, space engineering (including shipbuilding), metallurgical and chemical industries. However, there is no clear definition of the concept of "enterprises of strategic importance for the state economy and security" in the legislation.

Scientists propose to consider enterprises of strategic importance as ensuring the economic independence of the country, its statehood. R. Prokopiev proposes to define an enterprise that is of strategic importance for the economy and security of the state as a business entity of the public sector of the economy, which owns or holds objects of state property, including the corporate rights of the state in the authorized capital of business entities and which is responsible for at least one of criteria determined by the legislation of Ukraine on the specified legal relations, and/or in the prescribed manner included in the list of enterprises of strategic importance for the state economy and security [23].

The concept of "strategically important enterprise" is revealed in the studies of A. L. Balanda, V. P. Pavlenko, O. Iu. Rudchenko as an enterprise whose activities have a significant impact on the national economy safety and efficiency, its innovative development, as well as the livelihoods of the population through the implementation of scientific and technical, innovative, export, infrastructure potential, the production of progressive, socially significant or import-substituting products due to the presence of special operating conditions or a strategic effect as the ability to obtain an economic effect or prevent losses due to the inability to realize the interests of the future development of an enterprise or a relevant field of activity [24].

A number of scientists consider strategically important for the state defense, security and economy such enterprises that contribute to the national interests implementation and national security requirements in the military, social, economic, scientific and technological, environmental

or other fields due to the presence of a strategic effect as the ability to provide a dominant long-term impact on the situation in a certain industry (region, market) [25].

The main disadvantage of certain scientific approaches is the inclusion in strategically important enterprises of exclusively subjects of economic state ownership. It is while the majority of high-tech and innovative enterprises are privately or collectively owned.

In view of the foregoing, it is proposed to classify as strategically important enterprises of any form of ownership that produce critically important, unique products (works, services), which activities have a significant impact on the protection of national economic interests and the level of both the national economy and the country as a whole.

The lack of a unified scientifically based approach not only to the interpretation of the content, but also to the definition of the category that characterized strategically important enterprises, the imperfection of the current legislation are the main reasons for the lack of an effective mechanism for state regulation of the strategically important enterprises activities in terms of ensuring national interests and the national economy security.

The basis for the development of effective forms of state regulatory policy implementation in the direction of ensuring the strategically important enterprises security is the existence of an effective institutional environment. Therefore, it is legitimate to determine the conceptual provisions of institutionalism and neo-institutionalism as a theoretical and methodological basis for studying the institutional support of state regulatory policy in the aspect of strengthening the security of strategically important enterprises.

Institutional approach, i.e. the study of the activity and interaction of economic agents through the prism of institutions, is recognized as a general research method, due to the emphasis on the structural and functional principles of construction and the formal legal characteristics of the economic system, it makes it possible to determine the interdependence and relationship between changes in institutional structures and the activities of economic agents [26].

The deepening of the conceptual principles of the institutional support of the state regulatory policy implies, first of all, the specification and systematization of the categorical apparatus.

The analysis of scientific approaches to the definition of the categories "institute" and "institution" enables to conclude that their economic content is homogeneous and the degree of consistency differs. It is legitimate to consider the institution as a system, while the institution is the institution basic indivisible element [27].

J. R. Commons, a representative of the "old institutionalism", characterizes institutions in a narrow sense, as "a system of laws or natural rights within which individuals act as prisoners" and in a broad sense – "collective action to control, liberalize and expand individual activity" [28]. The concept of "institutions", according to the approach of the founder of neo-institutionalism D. Nort, covers any kind of restrictions created with the aim of directing human interaction in a certain direction [29].

Summarizing the views of representatives of the "new institutionalism", it is advisable to define an institution as a system of norms and rules covering both formal and informal norms

that regulate relations between economic entities and imply the existence of appropriate organizational structures in order to achieve certain goals.

New institutionalism comprehends informal institutions as complementary to formal ones. According to D. North's approach, formal institutions are rules formed by people, laws and constitutions issued by the state and approved by parliaments, while informal institutions are unwritten rules (customs, traditions, social conventions and codes of conduct). At the same time, unwritten rules are deeper than formal ones, often complement them and even effectively affect the economy if this influence manifests itself over a long period [30].

Institutions are a form of manifestation of institutions. The essential characteristics of this category can be both legal norms and the procedure for establishing links between them, "which enables to streamline (regulate) relations between subjects of law in order to give them a sustainable character, for which appropriate organizational structures and control bodies are created" [31]. The concept of "institution" is basic for the theory of institutionalism and denotes a certain custom, order adopted in society, as well as their consolidation through law or organization.

The contextual analysis enabled to define institutional support as a process of formation of institutions and institutions consolidated in the form of organizations (state bodies, enterprises, infrastructure), laws and rules in the process of the economy functioning market mechanism evolution.

Institutional security of strategically important enterprises can be legitimately considered as a set of state and non-state institutions that ensure the formation of legislative, organizational and economic conditions necessary for the implementation of an effective state regulatory policy in the direction of ensuring the strategically important enterprises security.

As part of the institutional support of the state regulatory policy, it is advisable to distinguish two components:

- institutional and legal support is a normative form of functions implementation of state and non-state institutions in the direction of ensuring the security of strategically important enterprises;
- institutional and organizational support is a system of organizations (authorities) that ensure the formation of effective forms of state regulatory policy implementation in the direction of ensuring the strategically important enterprises security.

To date, the system of legal acts regulating the activities of strategically important enterprises in Ukraine includes the Decree of the Cabinet of Ministers of Ukraine "On determining the criteria for classifying state-owned objects as having strategic importance for the state economy and security" dated November 03, 2010 and Decree of the Cabinet of Ministers of Ukraine "On approval of the list of state-owned objects of strategic importance for the state economy and security" dated March 4, 2015.

As has been mentioned above, none of the legislative acts defines the concept of "strategically important enterprises", and the criteria for classifying business entities as such are exclusively quantitative (product share on the market, average number of full-time employees, volume of taxes paid) and they are based on belonging to a certain industry branches. Supporting the opinion of a number of scientists [24, 25], given the significant shortcomings of quantitative indicators

in the context of the dynamics of changes in the national and world economies, it is believed that the criteria for determining strategically important enterprises should be supplemented with qualitative indicators. Qualitative characteristics, determined by an expert, enable to establish the value of an enterprise for protecting national economic interests and strengthening the competitiveness and the national economy security. In the context of the war launched by the Russian Federation against Ukraine, this task is of strategic importance. The identification of enterprises that can increase the national space security, including the economic one, strengthen the country's defense potential and the implementation of the state regulatory policy to support their operation is the basis for ensuring national security.

As for the institutional and organizational support, there is no specially authorized body responsible for implementing the state regulatory policy of supporting and strengthening the strategically important enterprises security. The lack of clear coordination and distribution of functional responsibilities among public authorities complicates the formation of an effective mechanism for state regulation of strategically important enterprises.

Thus, the institutional environment for ensuring security strategically important enterprises in Ukraine can definitely be considered undeveloped. In order to form effective forms of the state regulatory policy implementation to support and strengthen the strategically important enterprises security, a number of measures must be taken.

1. To develop scientifically based legal approach to granting the status and determining the features of the functioning of strategically important enterprises, which provides for the legislative consolidation of the concept of "strategically important enterprises" and the addition of criteria for classifying business entities to this category with qualitative indicators.

2. To improve the institutional and organizational support of the state regulatory policy to maintain and strengthen strategically important enterprises security, which determines the need to create a specially authorized body and conduct systematic monitoring of the strategically important business entities functioning.

3. To carry out clustering of the national economy based on strategically important enterprises with the ability to form integrated corporate structures, which increase the level of competitiveness and the national economy security, and minimize threats to national interests.

Institutional provision of economic security in Ukraine requires clarification in determining the forms, relationships, mutual influences of components, carrying out transformations to increase its level. Thus, special attention requires the search for new methods, forms and means of the level of economic security regulating.

It is worth noting that currently there is no normative definition of the concept of economic security of either an enterprise or any other form of doing business in the current legislation of Ukraine. However, in Ukraine there are separate legislative acts regulating certain aspects of the enterprises economic security. In particular, the Law of Ukraine "On the basic principles of state supervision (control) in the field of economic activity", which defines the general principles of state supervision (control) over compliance with the law in the field of economic activity, as well as the

Law of Ukraine "On the protection of economic competition", which determines the procedure for preventing unfair competition and ensuring equal conditions for all market players. At the same time, there is no clear definition of the category "economic security of a business entity" in the national legislation. In this regard, the problem of the lack of precise criteria and indicators of both economic security of economic structures state one remains, which could be used at the state level to monitor and control the economic security level.

Considering the experience of the EU, let's note that the security of economic entities of the EU countries is regulated by a number of legal acts, which include: Regulation (EU) 2016/679 on the protection of individuals regarding the processing of their personal data and the free movement of such data; Directive (EU) 2016/943 on the protection of know-how and confidential information; Directive (EU) 2019/770 on certain aspects of the implementation of electronic commerce in the internal market; Regulation (EU) 2019/1020 on ensuring the free movement of goods on the internal market; Directive (EU) 2014/95 on the disclosure of mistreatment, environmental liability and social behavior.

As for the practical experience of the EU member states in terms of ensuring the economic security of business entities, in Germany one of the ways to determine the level of economic security of enterprises is to use various business models and rating systems. For example, Deutsche Bank assesses the financial performance of enterprises and assigns them a rating that reflects their level of economic security. In addition, there are special rating agencies, such as Creditreform and Euler Hermes, which also assess risks and assign ratings to enterprises [31]. There is also a special economic reporting system that obliges businesses to publish their financial statements and other information about their activities. This allows assessing the financial stability and efficiency of enterprises and determining their level of economic security level.

The country has developed a regulatory framework that regulates the issues of ensuring the enterprises economic security. In particular, according to the Restriction of Competition Act (GWB), the German government has the right to inspect and control the activities of enterprises in matters of competition, as well as to prevent and eliminate the consequences of negligence and abuse in the economic sphere. The Bankruptcy and Reorganization Act (InsO) establishes rules and procedures for the event that an enterprise cannot pay its obligations to creditors and provides for the possibility of reorganizing an enterprise in order to maintain its activities and prevent bankruptcy. The Personal Data Protection Act (DSGVO), which establishes the rules for the collection, storage and use of personal data, is aimed at protecting private information and ensuring the security of data processing [32].

In addition, there are special bodies that are engaged in ensuring economic security at different levels. For example, the Federal Agency for Technical Supervision (TÜV) checks the technical safety of products and equipment used in factories; The Federal Occupational Safety Agency ensures the safety and health of workers in the workplace.

It is important to note that the legal and regulatory framework for the security of economic agents in Germany is quite developed and complex, and includes not only federal laws, but also the laws of individual states, regulations, standards and recommendations.

In France, at the level of state security agencies, which include, in particular, the Ministry of the Interior, the Ministry of Economy and Finance, the Ministry of Defense and others, monitoring and analysis of economic risks and threats are carried out. They monitor changes in the market, track financial and economic risks, and study the situation in sectors of the economy that are critical to national security [33].

In addition, the responsibility for ensuring economic security exists with the enterprises themselves. Enterprises can independently analyze the economic security level and conduct internal audits. There are a number of regulations that establish requirements for organizing the activities of enterprises in order to ensure economic security. In particular, it applies to the Laws on the Modernization of the Economy (Loi de modernisation de l'économie) of August 4, 2008, which contains provisions to promote competition, reduce bureaucracy and improve the regulation of enterprises; "On the protection of enterprises and their territorial integrity" (Loi de sauvegarde des entreprises et de leurs territoires) of August 6, 2015, containing provisions on protecting enterprises from bankruptcy, supporting both small and medium-sized enterprises, developing economically underdeveloped regions and providing conditions for creating new jobs; "On financial security" (Loi de sécurité financière) of August 1, 2003, containing provisions for ensuring the financial stability and reliability of the financial market functioning, regulating the activities of financial institutions and protecting investors [34].

These regulations are designed to ensure the economic security of businesses in France, as well as to increase their competitiveness and sustainability. They establish rules and requirements for the activities of enterprises in various industries, which helps to increase the efficiency of activities and reduce possible risks.

In addition, there are a number of tools helping enterprises to determine and ensure their economic security. In particular, the French Association of Entrepreneurs and Employers (MEDEF) analyzes economic risks and threats at the level of the national economy and develops proposals for state policy in the economic security field not only government agencies, but also private companies, since it is important for ensuring the sustainable development of the economy as a whole.

Ensuring the economic security of enterprises in France is based on the interaction of both state bodies and business entities.

An important role in ensuring the economic security of enterprises in Poland is played by legal acts regulating the functioning of business and ensuring its protection. Such acts include the Code of Economic Law (Kodeks Spółek Handlowych), which establishes the rules for the implementation of economic activities, as well as the protection of the entrepreneurs's rights in court; the Law on Protection of Competition (Ustawa o ochronie konkurencji i konsumentów), which purpose is to prevent unfair competition and ensure equal conditions for all market players; Enterprise Support Law (Ustawa o wspieraniu przedsiębiorczości), establishing support mechanisms for small and medium-sized enterprises, enabling them to remain competitive and grow [35].

In addition, Poland has state programs and projects aimed at ensuring the economic security of enterprises. Thus, the National Program for the Support of Small and Medium Business Go to

Brand aims to increase the competitiveness of Polish companies and promote their development, which is the basis for safe operation.

In Poland, the issues of economic security of enterprises are dealt with by various state bodies and institutions. In particular, the activities of the Ministry of Development, Labor and Technology (Ministerstwo Rozwoju, Pracy i Technologii) are aimed at ensuring the development of the country's economy, creating favorable conditions for business development; National Bank of Poland (Narodowy Bank Polski) deals with implementation of monetary policy, stabilization of the financial system and protection of the interests of economic agents; Entrepreneurship and Innovation Committee (Komitet do Spraw Przedsiębiorczości and Innowacyjności) develops and implements legislative acts aimed at supporting the development of entrepreneurship and innovation in the country. These institutions are effectively cooperating in the direction of ensuring the economic security of Polish enterprises.

Considering the European experience in ensuring the enterprises economic security, it is possible to formulate a number of recommendations for Ukraine: developing a comprehensive plan for ensuring the enterprises economic security, including the necessary regulatory acts and mechanisms to ensure their implementation; creating a centralized state structure responsible for enterprises economic security ensuring and coordination the activities of other state bodies; establishing transparent business rules for businesses, including protecting the rights of entrepreneurs in court and preventing unfair competition [36]; developing support mechanisms for both small and medium-sized enterprises in order to maintain their competitiveness and growth.

3.4 MODELING THE PROCESS OF EVALUATING THE STATE REGULATORY POLICY EFFECTIVENESS FOR ENSURING STRATEGICALLY IMPORTANT ENTERPRISES STRATEGY

Efficiency is a complex economic category that reflects the ratio between the obtained results resources spent to achieve them. The content of the efficiency category is complex and multi-faceted: there is no single definition of this concept.

The concept of "efficiency" is often identified with the category of "effectiveness". It due to the fact that efficiency from the Latin *efectus* means result, effectiveness or efficiency. At the same time, these terms are not identical. Based on this, the task of more accurate economic identification of the efficiency category arises.

According to the classical definition of efficiency, the minimum advance of capital should lead to the maximum surplus value. In modern conditions, this definition does not reflect the whole essence and content of the concept of "efficiency". Like other most general categories of economic science, the concept of efficiency is constantly evolving, and its content is gradually changing and becoming more complex.

Some economists consider efficiency as the ability to bring an effect, the effectiveness of a process, project, etc., which are defined as the ratio of the effect, result to the costs that

ensured this result [37]. In turn, the effect is the result achieved in various forms of manifestation (material, monetary, social, etc.).

Many economists support the definition of efficiency as the effectiveness of a certain action, process measured by the ratio between the obtained result and the costs (resources) that caused it [38].

In the works of W. Kip Viscusi, J. M. Vernon and J. E. Harrington, devoted to the economic theory of regulation, the effectiveness of regulatory policy is measured by maximizing the net benefits that regulatory measures can bring to society [39].

Thus, the state regulatory policy effectiveness can be legitimately defined as the ability to ensure the national economy development and improve the welfare of citizens based on balancing the interests of business entities, society and the state.

The state regulatory policy effectiveness depends on the economic feasibility and effectiveness of regulatory measures. Regulatory measures are proposed to be understood as measures that are carried out by regulatory authorities through the adoption of relevant regulatory acts and are aimed at ensuring the socio-economic development of both the country and regions, improving the welfare of citizens [40].

Considering the provisions of the current regulatory framework in the field of state regulatory policy implementation, it is legitimate to note the following. The Law of Ukraine "On the Fundamentals of the State Regulatory Policy in the Sphere of Economic Activity" defines efficiency as one of the principles of the state regulatory policy. At the same time, the regulatory policy effectiveness is defined as ensuring that, as a result of the regulatory act, the maximum possible positive results are achieved at the expense of the minimum necessary expenditure of economic entities, citizens and the state.

It is legitimate to determine the following criteria for the effectiveness of the state regulatory policy implementation:

1. Efficiency – the degree of achievement of both tactical and strategic goals.
2. Economic feasibility – the degree of resources usage in the process of achieving the set goals.
3. Quality – the level of compliance with legally established requirements for the production order.

Summarizing approaches to the interpretation of the concept of "efficiency", it can be argued that efficiency is a complex category, which is formed under the influence of a combination of both external and internal factors. In this regard, the process of evaluating the effectiveness of the state regulatory policy implementation requires a comprehensive and balanced approach.

Since efficiency is a multi-vector and diverse category, its evaluation is a tool that can be used to determine how the state regulatory policy implementation corresponds to the level of the country's strategic goals, the level of the national economy development.

The study and generalization of domestic and foreign methods and techniques for assessing the effectiveness of the state regulatory policy development enabled to develop a methodology for assessing the effectiveness of the state regulatory policy implementation, based on balancing the interests of stakeholders: the state, business entities and citizens. The process of evaluating

the effectiveness of the state regulatory policy implementation includes a number of successive stages (Fig. 3.5).

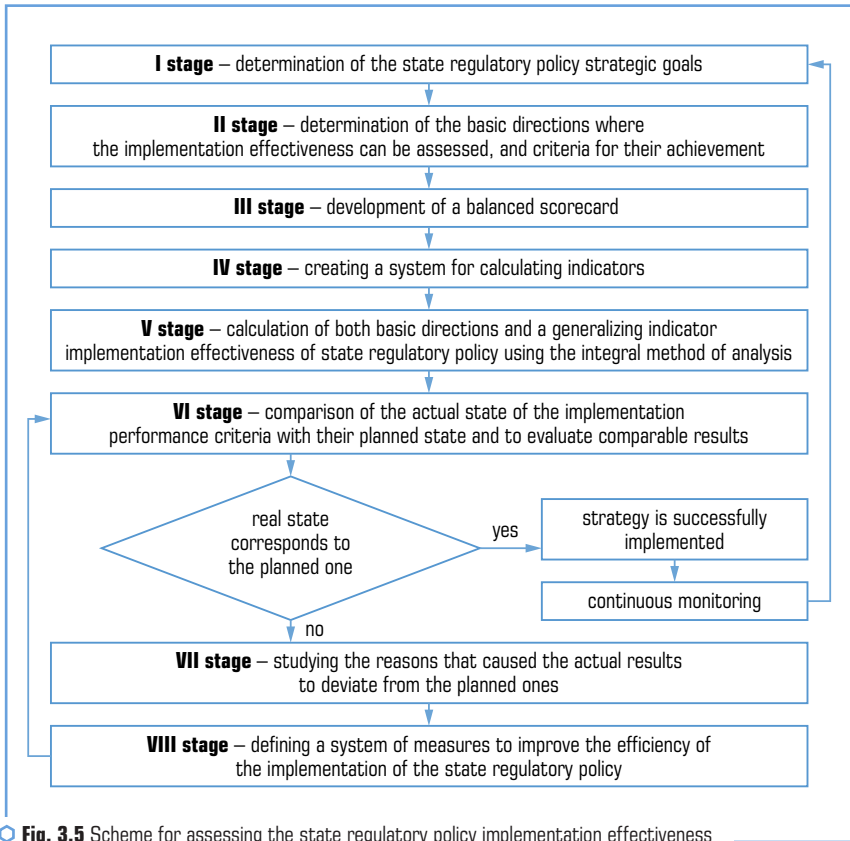


Fig. 3.5 Scheme for assessing the state regulatory policy implementation effectiveness
 Note: compiled by the author

At the first stage, the strategic goals of the state regulatory policy are determined considering the interests of the state (ensuring the growth of the national economy and its competitiveness in the world market), business entities (profit maximization) and citizens (improving living standards and ensuring the social guarantees implementation).

The second stage of the algorithm for evaluating the effectiveness of the state regulatory policy implementation also involves the definition of performance criteria. In a general sense, criteria is a sign on which basis the quality of both economic objects and processes has been assessed, alternatives have been compared, and objects and phenomena have been classified.

Thus, the criterion of implementation efficiency should be understood as either a sign or a set of signs, on which basis the current level of efficiency in the state regulatory policy implementation and the ability to improve it have been determined. Such criteria should include, in particular, the growth of gross domestic product at the macro level and the growth of revenues of business entities at the micro level.

As a part of the third stage, a system of evaluation indicators has been developed and approved for each direction, and causal relationships of indicators, areas of implementation and criteria for their evaluation have been determined.

The selection of indicators is quite important, since the reliability of the results assessing the effectiveness of the state regulatory policy implementation depend on their objectivity and comprehensiveness. The formation of a system of indicators at the macro level has been legitimately carried out on the basis of a representative sample in terms of the development indicators of the production, financial, investment, foreign economic, scientific and technological, energy and social spheres, and at the micro level – according to the indicators of the business sector. In this case, it is advisable to use a typical selection method, which provides for a preliminary distribution of the general population into relatively homogeneous categories, from which a random sample is then proportionally carried out.

At the fourth stage, algorithms for calculating the estimated indicators for each direction have been determined. Since the comprehensive methodology for assessing the effectiveness of the implementation of the state regulatory policy includes both quantitative and qualitative indicators, the definition of quantitative indicators is carried out by applying the appropriate formulas based on statistical data, and qualitative indicators – by applying scoring based on the expert survey method.

The estimation of both basic directions effectiveness and the generalizing indicator effectiveness of the state regulatory policy implementation using the integral method of analysis has been carried out as a part of the fifth stage.

The next step is to compare the actual state of the implementation efficiency criteria with their planned state, as well as evaluate the results of the comparison. If the actual level corresponds to the planned one, then the regulatory activity of the authorities is directed to support or increase. Otherwise, there is a transition to the seventh stage, at which the study of the reasons for the unsatisfactory state of the efficiency of the implementation of state regulatory policy is carried out.

The final stage provides for the determination of a system of measures to improve the efficiency of the state regulatory policy in the areas indicated above.

Thus, the assessment of the effectiveness of the implementation of the state regulatory policy is the basis for increasing its level. The maximum effect is possible only with a comprehensive and systematic approach to the implementation of regulatory measures and mandatory monitoring of their effectiveness, which should be carried out directly by the regulatory authorities. A special role in ensuring the effectiveness of the implementation of state regulatory policy belongs to the State Regulatory Service of Ukraine and its territorial offices.

CONCLUSIONS

The assessment of the Ukrainian economic security level indicates the need to strengthen it, primarily through the revitalization of business entities. Deregulation of entrepreneurial activity is the basis for both efficient and stable functioning of business in Ukraine. In this aspect, considering the key provisions of the Draft Ukraine Recovery Plan, it is advisable to determine the following strategic directions for deregulating business activities in Ukraine.

1. Spreading the declarative principle of entrepreneurial activity with the simultaneous transformation of the state supervision system (reorientation from controlling to service approaches, increasing the level of advisory support to business entities).
2. Creation of the Unified register of permits and transfer of all licenses and permits in electronic form, especially in the territories where hostilities are taking place.
3. Introduction of a declarative principle for permits for construction work at industrial facilities, as well as construction work for the creation of processing enterprises in agriculture on agricultural land.
4. Spreading the practice of digitalization of public services and full digitalization of licensing and licensing procedures.
5. Increasing the level of involvement of business entities in the processes of development and decision-making aimed at simplifying the regulatory environment (in particular, the development of regulatory acts, their discussion and revision, which is provided for by the provisions of the Law of Ukraine "On the fundamentals of state regulatory policy in the field of economic activity").
6. Improving the mechanism for protecting business from the state (institutionalization of the Business Ombudsman Council, resuming the survey of business entities ABCA (Annual Business Cost Assessment) considering their interests).
7. Ensuring the effective operation of the Economic Security Bureau as a key body in the field of combating economic crimes.

Deregulation of entrepreneurial activity is the basis for business both efficient and stable functioning in Ukraine. The implementation of regulatory tools to support and develop the national economy should be systematic and consistent and based on the principles of creating a favorable regulatory environment. In order to restore the national economy, it is necessary to further reduce the regulatory and administrative burden on business by introducing deregulation measures based on a risk-based approach for the development of business self-regulation, which involves the formation of a transparent licensing system and the development of partnerships between economic entities and state regulatory authorities. Considering the European integration course of Ukraine, it is legitimate to determine the study of the experience of the EU countries in the regulatory environment formation and its implementation in Ukraine as a promising direction for further research.

In the conditions of war, the objective condition for strengthening the country's defense capability, supporting and restoring the economy, strengthening the security of the national space and protecting national interests is legitimately determined to ensure the operation and security of

strategically important enterprises. Considering that security is implemented by business entities, at the same time, the need to create a favorable institutional environment, which is the prerogative of public authorities, has been noted. In this context, an analysis of the existing institutional support of the state regulatory policy in relation to strategically important enterprises has been carried out. The basis for the formation of effective forms of the state regulatory policy implementation of support and strengthening the security of strategically important enterprises is the need to improve the current legislation, the formation of effective institutional and organizational support and the clustering of the national economy on the basis of strategically important enterprises with the possibility of creating integrated corporate structures.

The proposed model of the evaluation process provides the regulatory authorities with a tool to influence the level of efficiency in the implementation of the state regulatory policy to ensure the safety of strategically important enterprises. The main advantages of the process proposed model for assessing the effectiveness of the state regulatory policy implementation can be legitimately identified as follows:

- 1) it is based on an integrated approach to assessing such a complex phenomenon as efficiency;
- 2) the main sources of information are official statistics;
- 3) it contains both quantitative and qualitative indicators;
- 4) it is not well-established and may change directions depending on the purpose of the analysis.

In general, the obtained results are the basis for the formation and implementation of the state regulatory policy in the direction of strengthening the strategically important enterprises security in the future ensuring economic development and social stability in Ukraine in the future.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Pro zatverdzhennia Metodychnykh rekomendatsii shchodo rozrakhunku rivnia ekonomichnoi bezpeky Ukrainy (2013). Nakaz Ministerstva ekonomichnoho rozvytku i torhivli Ukrainy No. 1277. 10.29.2013. Available at: <https://zakon.rada.gov.ua/rada/show/v1277731-13#Text>
2. State Statistics Service of Ukraine. Available at: <https://www.ukrstat.gov.ua/>
3. Onyshchenko, S., Shchurov, I., Cherviak, A., Kivshyk, O. (2023). Methodical approach to assessing financial and credit institutions' economic security level. *Financial and Credit Activity Problems of Theory and Practice*, 2 (49), 65–78. doi: <https://doi.org/10.55643/fcaptp.2.49.2023.4037>

4. Glushko, A. D. (2013). Directions of Efficiency of State Regulatory Policy in Ukrain. *World Applied Sciences Journal*. Pakistan: International Digital Organization for Scientific Information, 27 (4), 448–453.
5. Onyshchenko, S., Bilko, S., Yanko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). *Business Information Security Proceedings of the 4th International Conference on Building Innovations*. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 769–778. doi: https://doi.org/10.1007/978-3-031-17385-1_65
6. Pidsumky 2022 roku ta ochikuvannia shchodo 2023 roku. National Institute for Strategic Studies. Available at: <https://niss.gov.ua/news/komentari-ekspertiv/pidsumky-2022-roku-ta-ochikuvannya-shchodo-2023-roku>
7. Shpachuk, V., Hornyk, V., Kravchenko, S., Vizirov, B., Aleinikova, O., Abuselidze, G. (2023). State policy of cooperation between countries and global institutions: condition and prospects. *E3S Web of Conferences*, 371. doi: <https://doi.org/10.1051/e3sconf/202337105004>
8. Information on the regulatory activities of the Ministry of Economy for 9 months of 2022. Available at: <https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=33c54edf-ce57-4df7-a0bf-c1808ac12e26&title=InformatsiiaSchodoZdiisnenniaRegulatornoiDiialnostiMinekonomikiZa9-Misiatsiv2022-Roku>
9. Glushko, A., Marchyshynets, O. (2018). Institutional Provision of the State Regulatory Policy in Ukraine. *Journal of Advanced Research in Law and Economics*, 9 (3), 941–948. doi: [https://doi.org/10.14505/jarle.v9i3\(3\).18](https://doi.org/10.14505/jarle.v9i3(3).18)
10. Ohliad instrumentiv pidtrymky biznesu v period dii voiennoho stanu v Ukraini (za 01.05 – 31.05.2022 r.) (2022). National Institute for Strategic Studies. Available at: <https://niss.gov.ua/news/komentari-ekspertiv/ohlyad-instrumentiv-pidtrymky-biznesu-v-period-diyi-voyennoho-stanu-v>
11. Uriad zapuskaie prohramy hrantiv dlia rozvytku pidpriemnytstva ta navchannia ukraintsiv (2022). Government portal. Available at: <https://www.kmu.gov.ua/news/uryad-zapuska-ye-programi-grantiv-dlya-rozvytku-pidpriemnictva-ta-navchannya-ukrayinciv>
12. Prohrama relokatsii: 761 pidpriemstvo peremishcheno v bilsh bezpechni rehiony. Ministry of Economy of Ukraine. Available at: <https://www.me.gov.ua/News/Detail?lang=uk-UA&id=d-152dcfe-7bde-49df-a69a-8d7f9586fc13&title=ProgramaRelokatsii>
13. Minfin: Za chas dii voiennoho stanu v mezhakh Derzhavnoi prohramy "Dostupni kredyty 5-7-9 %" vydano 17 359 pilhovyykh kredytiv na 72,24 mlrd hrn (2022). Available at: https://mof.gov.ua/uk/news/minfin_za_chas_dii_voiennogo_stanu_v_mezhakh_derzhavnoi_programi_dostupni_krediti_5-7-9_vidano_17_359_pilgovikh_kredytiv_na_7224_mlrd_gm-3782
14. Onyshchenko, S., Brychko, M., Litovtseva, V., Yevsieieva, A. (2022). Trust in the financial sector: a new approach to conceptualizing and measuring. *Financial and Credit Activity Problems of Theory and Practice*, 1 (42), 206–217. doi: <https://doi.org/10.55643/fcaptop.1.42.2022.3735>

15. PryvatBank pryiednavsia do partnerskoi prohramy Eksportno-kredytnoho ahentstva (2022). Available at: <https://finclub.net/ua/news/pryvatbank-pryiednavsia-do-partnerskoi-prohramy-eksportnokredytnoho-ahentstva.html>
16. Mizhnarodna finansova korporatsiia profinansuie kredytuvannia ukrainskoho biznesu na 2 mlrd dolariv (2022). Ministry of Economy of Ukraine. Available at: <https://www.me.gov.ua/News/Detail?lang=uk-UA&id=3cd7a0de-bfd7-4cba-b08e-d3ebdda176aa&title=MizhnarodnaFinansovaKorporatsiiaVidilila2-MlrdDolarivNaPidtrimkuInvestitsiiVUkrainu>
17. Minfin: Fond rozvytku pidpriemnytstva profinansuie investytsii MSP u sferi enerhozabezpechennia ta enerhoefektyvnosti spilno z AB "UKRHABANK" (2022). Ministry of Finance of Ukraine. Available at: <https://www.kmu.gov.ua/news/minfin-fond-rozvytku-pidpriemnytstva-profinansuie-investytsii-msp-u-sferi-enerhozabezpechennia-ta-enerhoefektyvnosti-spilno-z-ab-ukrhazbank>
18. Stan ta potreby biznesu v umovakh viiny: rezultaty opytuvannia v lystopadi 2022 roku (2022). Diia Business. Available at: <https://business.diia.gov.ua/cases/novini/stan-ta-potrebi-biznesu-v-umovah-vijni-rezultati-opytuvanna-v-listopadi-2022-roku>
19. eRobota: 136 ukraintsiiv otrymauiut mikrohranty vid derzhavy na vlasnu spravu (2023). Government portal. Available at: <https://www.kmu.gov.ua/news/yerobota-136-ukraintsiiv-otrymauiut-mikrohranty-vid-derzhavy-na-vlasnu-spravu>
20. Uriad zapuskaie hrantovi prohramy dlia veteraniv u mezhakh eRobota, – Denys Shmyhal (2023). Government portal. Available at: <https://www.kmu.gov.ua/news/uriad-zapuskaie-hrantovi-prohramy-dlia-veteraniv-u-mezhakh-ierobota-denys-shmyhal>
21. Za chas dii voiennoho stanu v mezhakh Derzhavnoi prohramy "Dostupni kredyty 5-7-9 %" vydano 23 999 pilhovyykh kredytiv na sumu blyzko 96 mlrd hrn (2023), Ministry of Finance of Ukraine. Available at: https://www.mof.gov.ua/uk/news/minfin_za_chas_dii_voiennogo_stanu_v_mezhakh_derzhavnoi_programi_dostupni_kredyty_5-7-9_vidano_23_999_pilgovikh_kredytiv_na_sumu_maizhe_96_mlrd_grn-3904
22. Onyshchenko, S., Maslii, O., Kivshyk, O., Cherviak, A. (2023). The Impact of the Insurance Market on the Financial Security of Ukraine. *Financial and Credit Activity Problems of Theory and Practice*, 1 (48), 268–281. doi: <https://doi.org/10.55643/fcaptive.1.48.2023.3976>
23. Prokopiev, R. (2023). Enterprises having strategic value for economy and safety: problems of legal regulation. *Bulletin of the Academy of Legal Sciences of Ukraine*, 1, 262–270. Available at: http://nbuv.gov.ua/UJRN/vapny_2013_1_28
24. Balanda, A. L., Pavlenko, V. P., Rudchenko, O. Yu. (2016). Institutional ensuring of state regulation of strategically important enterprises for economy and security of state. *Formation of market relations in Ukraine: a collection of scientific papers*, 5 (180), 18–22. Available at: http://nbuv.gov.ua/UJRN/frvu_2016_5_7
25. Mantsurov, I., Rudchenko, O., Novikov, V. (2017). Fenomen stratehichno vazhlyvykh pidpriemstv v Ukraini. *Ukraine: aspects of labor*, 3, 44–51. Available at: https://ir.kneu.edu.ua/bitstream/handle/2010/32761/1_UAP3_17.pdf

26. Onyshchenko, S., Skryl, V., Hlushko, A., Maslii, O.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). Inclusive Development Index. Proceedings of the 4th International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 779–790. doi: https://doi.org/10.1007/978-3-031-17385-1_66
27. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. *International Journal of Engineering & Technology*, 7 (3.2), 447–452. doi: <https://doi.org/10.14419/ijet.v7i3.2.14569>
28. Commons, J. R. (1931). Institutional Economics. *American Economic Review*, 21, 648–657. Available at: <http://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/commons/institutional.txt>
29. North, D., Mantzavinos, C., Shariq, S. (2003). Learning, Institutions, and Economic Performance. Discussion Paper Series of the Max Planck Institute for Research on Collective Goods, 1, 75–84. Available at: http://www.coll.mpg.de/pdf_dat/2003_13online.pdf
30. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 791–803. doi: https://doi.org/10.1007/978-3-031-17385-1_67
31. German Federal Ministry for Economic Affairs and Energy. Available at: <https://www.bmwi.de/Redaktion/DE/Home/home.html>
32. German statistical offices research "Indicators of Economic Security". Available at: <https://www.destatis.de/EN/Themes/Society-Environment/Quality-Life/Indicators-of-Economic-Security/Indicators-of-Economic-Security.html>
33. Ministry of Economy and Finance of France. Available at: <https://www.economie.gouv.fr/>
34. French legislation. Available at: <https://www.legifrance.gouv.fr/>
35. Ministry of Enterprise and Technology of Poland. Available at: <https://www.gov.pl/web/entrepreneurship-and-technology-ministry>
36. Onyshchenko, S., Hlushko, A., Kivshyk, O., Sokolov, A. (2021). The shadow economy as a threat to the economic security of the state. *Economics of Development*, 20 (4), 24–30. doi: [https://doi.org/10.57111/econ.20\(4\).2021.24-30](https://doi.org/10.57111/econ.20(4).2021.24-30)
37. Pelagidis, T., Mitsopoulos, M. (2019). In Defense of Making Things: Why Manufacturing Still Matters. *Relations Industrielles*, 74 (1), 187–192. doi: <https://doi.org/10.7202/1059471ar>
38. Ansoff, I., Kipley, D., Lewis, A., Helm-Stevens, R., Ansoff, R. (2018). *Implanting strategic management*. Cham: Palgrave Macmillan, 592. doi: <https://doi.org/10.1007/978-3-319-99599-1>
39. Viscusi, W. K., Vernon, J. M., Harrington, Jr. J. E. (2005). *Economics of Regulation and Antitrust*. The MIT Press, 960.
40. Onyshchenko, S., Onyshchenko, V., Verhal, K., Buriak, A. (2023). The Energy Efficiency of the Digital Economy. Lecture Notes in Civil Engineering, 299, 761–767. doi: https://doi.org/10.1007/978-3-031-17385-1_64

Kateryna Potapova, Mykola Nalyvaichuk, Vasyl Meliukh,
Stanislav Guryenko, Kostiantyn Koliada, Alexandre Scherbyna
© The Author(s) 2023

CHAPTER 4

SEMANTIC ROLE LABELLING AND ANALYSIS IN ECONOMIC AND CYBERSECURITY CONTEXTS USING NATURAL LANGUAGE PROCESSING CLASSIFIERS

ABSTRACT

Semantic Role Labeling (SRL) is a crucial task in Natural Language Processing (NLP) that plays a vital role in extracting meaningful information from text. In the fields of economics and cybersecurity, accurately identifying and analyzing semantic roles within text is crucial due to the rapid increase in the amount and complexity of textual information. This abstract examines the significant role of SRL and its application in economic and cybersecurity contexts. It discusses the state-of-the-art NLP classifiers used for this purpose. By examining the relationship between language processing and these important areas, we aim to emphasize the importance of SRL in extracting useful information and improving decision-making in a constantly changing digital environment.

The aim of the findings is to emphasize the significance of SRL in extracting valuable insights from text, as it serves as a fundamental technique in NLP. It is utilized in the economic context to analyze financial reports, news articles, and economic texts. It assists in decision-making and market analysis. It aids in identifying important participants, actions, and objects in economic discourse, leading to better decision-making and market analysis. In the field of cybersecurity, SRL assists parse and comprehending text data related to security, enabling faster responses to threats. NLP classifiers and machine learning models utilize SRL to automate the analysis of large amounts of text. These techniques are practically significant as they improve the ability to extract actionable insights, assess risks, and make informed decisions by organizing unstructured text data.

The process of determining relevant information from a large corpus of data requires an optimal methodological basis. Relevant textual data is collected from sources such as financial reports, news articles, or cybersecurity incident reports. Textual data is cleaned, tokenized, and tagged with part-of-speech labels in preparation for NLP analysis. Human annotators label semantic roles in the text, identifying actors, actions, and objects. This creates a dataset that can be used to train classifiers. NLP classifiers, including machine learning models, are trained using annotated datasets to identify semantic roles. The accuracy and performance of the trained classifiers are evaluated using various metrics. NLP classifiers are used to automatically identify and label semantic roles in new, unseen textual data. The output helps extract insights, such as market trends or security threats, depending on the specific field. Researchers improve classifier models by iteratively training and applying them to increase accuracy.

KEYWORDS

Semantic Role Labelling, NLP Techniques, Economic Data Analysis, Cybersecurity Text Mining, Semantic Role Extraction, Sentiment Analysis, Information Security.

In an age dominated by digital information and economic interdependence, the realms of economics and cybersecurity have gained unprecedented significance. The vast amount of textual data generated in these fields calls for advanced techniques to extract valuable information. Semantic Role Labelling (SRL) has emerged as a powerful Natural Language Processing (NLP) approach to analyze the complex relationships and roles of entities within text [1]. It aims to label words in a sentence with different semantic roles for the verb in the sentence. SRL has gained significant attention in computational linguistics and has become a leading task in the field [2]. It plays a crucial role in understanding the meaning and structure of sentences, enabling various downstream applications such as information extraction, question answering, and machine translation.

The significance of understanding the semantic roles in economic and cybersecurity texts cannot be overstated. In economics, we often deal with massive datasets, financial reports, and market sentiment analysis, where identifying roles like "buyer", "seller", "investor", or "regulator" is crucial for informed decision-making. By accurately identifying the semantic roles of predicates in these texts, NLP classifiers can assist in automating tasks such as sentiment analysis, trend prediction, and risk assessment. Similarly, in the cybersecurity context, SRL can be used to analyze security-related documents, incident reports, and online discussions to identify potential threats, vulnerabilities, and malicious activities. By understanding the semantic arguments of predicates in these texts, NLP classifiers can aid in detecting patterns, identifying key actors, and predicting future cyberattacks.

The use of NLP classifiers in these domains can provide valuable insights and assist in decision-making processes. The text discusses the importance of efficient inference and structured learning techniques for accurate labeling in SRL (Structured Learning). It emphasizes the need for efficient inference and structured learning to achieve accurate labeling. These techniques can enhance the accuracy and reliability of SRL classifiers in economic and cybersecurity applications [1].

One approach to SRL is the use of data-driven models based on supervised learning, which have become the method of choice for semantic role labeling [2, 3]. These models leverage neural architectures and adapt them to the SRL task. Lample et al. adapted a similar model used for Named Entity Recognition and applied it to the SRL task. This approach demonstrates the potential of leveraging neural networks for SRL in different domains [4].

To achieve accurate and reliable Semantic Role Labeling (SRL), it is essential to leverage existing resources such as annotated corpora of semantic roles and ontologies [4]. These resources provide valuable knowledge and semantic mappings that can improve the performance of NLP classifiers. It proposes a method that leverages WordNet's upper ontology mapping and PropBank-style Semantic Role Labeling (SRL) for parsing long texts. This approach demonstrates the potential of

integrating ontological knowledge into SRL classifiers for a more comprehensive analysis. Semantic Role Labelling and Analysis using NLP classifiers have significant potential to enhance decision-making and situational awareness. By accurately labeling semantic roles and analyzing the relationships between entities and predicates in texts, these classifiers can provide valuable insights and support decision-making processes in these domains.

4.1 CONVENTIONAL PARADIGMS OF EMPIRICAL AND RATIONAL APPROACHES TO THE AMBIGUITY OF LINGUISTIC DURING THE DEVELOPMENT OF NATURAL LANGUAGE PROCESSING

Conventional paradigms in empirical and rational approaches to the ambiguity of language during the development of natural language processing have been extensively studied in the field of computational linguistics and artificial intelligence. Researchers have explored various aspects of language processing, including statistical natural language processing, individual differences in language processing, unsupervised learning of morphological paradigms, and ambiguity resolution [5].

Early approaches to SRL relied on rule-based systems, although they have undergone significant changes over time. These systems had a limited scope and necessitated extensive linguistic expertise. The development of machine learning methods, especially deep learning, has transformed SRL by enabling models to learn from vast text corpora. With increased accuracy and scalability resulting from this change, SRL is now more suitable for a variety of fields, including economics and cybersecurity.

The aim of linguistic science, in contrast, is to be able to describe and explain the wide range of linguistic observations that we frequently come across in speech, writing, and other media. An essential part of this process is recognizing the connections between linguistic expressions and the outside world, the linguistic structures through which language expresses meaning, and the cognitive aspects of how people acquire, produce, and comprehend language [6]. It has been suggested that there are rules used to shape language utterances as a way to address the final issue with rules. This fundamental method has a long history that dates back at least 2000 years. However, in this century, it became more formal and rigorous as linguists delved into complex grammars that aimed to determine which utterances in a language were grammatically correct and which were not.

In the field of natural language processing, there has been extensive debate on the empiricist and rationalist approaches to language. While the empiricist approach stresses the value of experience and sensory information, the rationalist approach places more emphasis on the role of innate knowledge and mental structures in language acquisition [5, 6]. A rationalist approach completely dominated the fields of linguistics, psychology, AI, and natural language processing from around 1960 to 1985. In the context of artificial intelligence, rationalist ideas can be regarded as supporting the effort to develop intelligent systems by manually hand-programming a large amount of initial knowledge and reasoning processes into them in an effort to replicate what the human brain initially contains. The rationalist school of thought contends that universal grammar and natural linguistic talents make learning a language easier. They argue that humans are born with a set of cognitive

mechanisms that are unique to language and facilitate the process of language learning [6]. The theory of generative grammar contends that all languages share underlying syntactic features, which supports this point of view [7]. The rationalist approach also emphasizes the importance of reflection and introspective methods for language comprehension [8].

Conversely, empiricists argue that language acquisition is largely influenced by exposure to linguistic information and the statistical regularities present in the environment. According to them, language can be learned without the use of innate information or mental processes through a process of generalization and pattern recognition [9]. Empiricists emphasize the importance of corpora and data-driven methodologies in language research. They also emphasize how the linguistic environment influences the development of language [8, 9].

Both empiricist and rationalist approaches have had an impact on the field of natural language processing. The development of formal grammars and rule-based language processing systems was influenced by the rationalist perspective [10]. To analyze and produce language, these systems rely on explicit linguistic structures and rules. In contrast, the empiricist method has sparked the growth of statistical and machine learning methods for language processing [11]. These methods create predictions about language and learn patterns from large amounts of data. The fundamental principle of empiricist approaches, however, is to assume that the mind does not initially possess comprehensive collections of rules and guidelines specific to different aspects of language and other cognitive domains (such as theories of morphological structure, case marking, and so on), and that the mind instead develops over time. An empiricist approach to NLP contends that by selecting an appropriate generic language model and then determining the parameter values through statistical pattern recognition, we can acquire a deep and comprehensive understanding of the structure of language. An empiricist approach to NLP contends that by selecting a suitable general language model and then applying statistical, pattern recognition, and machine learning techniques to a vast amount of language data, we can learn the complex and extensive structure of language.

An NLP system must understand the structure of the text, typically to a sufficient extent to answer the question "Who did what to whom"? Conventional parsing algorithms simply attempt to answer this question by considering potential grammatical structures for a specific set of words within a specific category [12]. For instance, a typical NLP system will indicate that the sentence in **Fig. 4.1** has multiple syntactic analyses, also referred to as parses, based on a valid grammar. The given parse tree represents a complex sentence stating that the central bank raised interest rates in an attempt to manage inflation. This tree structure provides a visual representation of the grammatical and syntactic elements of the sentence, facilitating understanding of its hierarchical structure and the relationships between its various parts. A useful NLP system must be proficient in distinguishing between words with similar meanings and words with different categories, syntactic structures, and semantic scopes. However, when using symbolic NLP systems, expanding the language coverage to include obscure formulations actually leads to more unwanted interpretations for common phrases, and vice versa. This means that the goal of maximizing coverage while minimizing ambiguity is fundamentally incompatible.

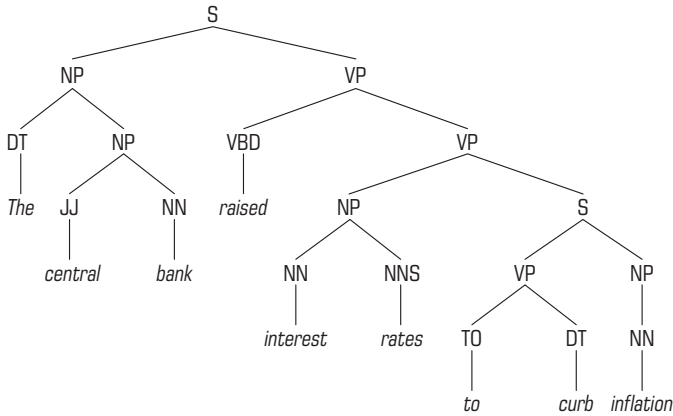


Fig. 4.1 A parse tree for a sentence "The central bank raised interest rates to curb inflation"

In the end, two opposing viewpoints on language learning can be seen in the rationalist and empiricist approaches to natural language processing. The empiricist method places more emphasis on the role of experience and statistical regularities than the rationalist approach, which emphasizes innate knowledge and mental structures. Both approaches have influenced the development of language processing tools, with empiricist approaches guiding the creation of statistical and machine learning techniques, and rationalist approaches influencing rule-based systems [13].

These issues are addressed by a statistical NLP technique that automatically learns lexical and structural preferences from corpora. Instead of relying exclusively on syntactic categories, such part of speech labels, to parse sentences, we understand that the associations between words – that is, which words tend to cluster together – contain a wealth of information [5, 8]. It is possible to use this collocational knowledge as a window into deeper semantic linkages. Because statistical models are stable, generalize well, and behave graciously in the presence of errors and new data, they are particularly useful for solving the ambiguity problem. In order to successfully provide disambiguation in large-scale systems that use naturally occurring text, statistical natural language processing (NLP) approaches have taken the lead. Statistical NLP models' parameters can often be automatically estimated from text corpora. This not only reduces the reliance on human labor in the development of NLP systems but also raises interesting scientific questions about the process of language acquisition in humans [5].

For groups of words W in a vocabulary V that number in the tens or hundreds of thousands, a statistical language model calculates the prior probability values $P(W)$. Typically, the string W is divided into sentences or other pieces that are presumed to be conditionally independent, like utterances in automatic speech recognition. Decomposing the sentence probability in accordance

with the chain rule and ensuring that the end-of-sentence symbol is predicted with a non-zero probability in any context are two straightforward and sufficient methods to ensure proper normalization of the model. $W = w_1, w_2, \dots, w_n$ results in:

$$P(W) = \prod_{i=1}^n P(w_i | w_1, w_2, \dots, w_{i-1}). \quad (4.1)$$

The language model is required to group the context $W_{k-1} = w_1, w_2, \dots, w_{k-1}$ into an equivalence class determined by a function $\Phi(W_{k-1})$ because the parameter space of $P(w_k | w_1, w_2, \dots, w_{k-1n})$ is too large. The result is:

$$P(W) \cong \prod_{i=1}^n P(w_i | \Phi(W_{k-1})). \quad (4.2)$$

In a real application, word strings of limited length are encountered. The support of $P(W)$ should consist of strings of finite length. The probability distribution $P(W)$ should assign a probability of 0.0 to strings of words of indefinite length. A language model must anticipate the specific end-of-sentence symbol since the text is divided into sentences in a real-world context. If the language model is straightforward, or in other words, if $P(w_k | \Phi(W_{k-1})) > \epsilon > 0, \forall w_k, W_{k-1}$, after that we have $P(\langle /s \rangle | \Phi(W_{k-1})) > \epsilon > 0, \forall W_{k-1}$. It guarantees that the model gives the set of word sequences with a fixed length a probability of 1.0 [13].

Finding appropriate equivalence classifiers and ways to assess the likelihood are the focus of language modeling research. The $(n-1)$ -gram equivalence classification, which defines $\Phi(W_{k-1})$, is the most effective paradigm for language modeling, leaving the problem of estimating probability from training, and it defined like that:

$$\Phi(W_{k-1}) = w_{k-n+1}, w_{k-n+2}, \dots, w_{k-1}. \quad (4.3)$$

Natural language processing (NLP) is one of the many fields where Zipf's law has been seen statistically. It claims that a word or term's rank is negatively correlated with how frequently it occurs in a corpus [14]. In other words, the majority of terms only occasionally occur, but a select minority do. For applications like semantic labeling, this law has been frequently used in NLP [11]. The generative modeling of natural languages is one area in which Zipf's law is applied in NLP. Researchers can create models that produce realistic and cohesive writing and get insights into the structure and qualities of a language by examining the frequency distribution of words in a corpus.

We can examine the correlation between the frequency of a word, denoted as f , and its position in a list, referred to as its rank, r , by tallying the occurrence of each word (type) in a large corpus. Subsequently, we can arrange the words in ascending order based on their frequency [13].

$$f \propto \frac{1}{r}, \text{ or } f = \frac{1}{r}. \quad (4.4)$$

Meaning that there is a constant k :

$$f * r = k, \quad (4.5)$$

$$f(r) = \frac{c}{(r + \beta)^\alpha}. \quad (4.6)$$

Its idea holds that both the speaker and the hearer are attempting to exert the least amount of effort possible. A short vocabulary of common words saves the speaker's effort, whereas a wide vocabulary of words that are individually rarer saves the hearer's effort by making communications less ambiguous. The kind of reciprocal relationship between frequency and rank that can be seen in the data proving Zipf's rule is said to be the most economically advantageous solution to these conflicting needs. The biggest impact of Zipf's law for us, nevertheless, is the practical issue that most words will have extremely scant usage data. We will only have a large number of samples for a few terms. As we can observe, Zipf's law roughly holds, however it varies significantly for the terms with the highest frequency. Additionally, a phenomenon that may be seen in many of Zipf's own research has been recognized, namely that the product f and r tend to show a tiny bulge for terms of higher ranks [5]. Although it is only a generalization, Zipf's law is helpful in describing the frequency distribution of words in human languages. It claims that there are a small number of highly common words, a substantial number of terms with medium frequency, and a significant number of words with low frequency.

The broader link between rank and frequency in order to achieve a better fit with the empirical distribution of words. that Mandelbrot discovers is as follows:

$$f = P(r + \rho)^{-B} \text{ or } \log f = \log P - B * \log(r + \rho). \quad (4.7)$$

P , B are text parameters that together gauge how varied the vocabulary is in the text. As in the original equation, there is still a hyperbolic distribution between rank and frequency. When this equation is plotted on logarithmic axes, it closely resembles Zipf's law as a declining straight line with slope B for large values of r . However, by appropriately selecting the other parameters, one can construct a curve where the expected frequency of the most common terms is lower.

4.2 ANNOTATING LINGUISTIC STRUCTURE

The act of parsing can be seen as a simple application of the concept of chunking, which allows to condense the description of a phrase by identifying higher level structural pieces. Learning a grammar that explains the structure of the chunks one encounters is one approach to grasp the regularity of chunks over various phrases. The issue with grammatical induction is this. The concept of syntactic constituency holds that word groups can function as single entities, or constituents. The process of creating a grammar includes creating a list of the language's components. Due to its

exploration of the empiricist challenge of how to acquire structure from unannotated textual input, grammar induction has received a lot of attention. It suffices to argue that, while context-free or more complicated languages of the size required to handle a respectable percentage of the complexity of human languages, grammar induction approaches are quite difficult to understand. It is simple to introduce organization into a corpus of text. A chunked representation of sentences, which we might understand as a phrase structure tree, will be produced by any algorithm for creating chunks, such as one that recognizes common subsequences. The process of mechanically examining a given sentence, seen as a sequence of words, in order to identify any potential underlying grammatical structures is known as parsing in the field of natural language processing [2].

Parsing requires a formal, grammar-based, mathematical representation of the syntax of the target language. A formal grammar is made up of a set of rules that define how language constituents, such as words, may be put together to make sentences and how sentences should be put together. The subject-verb agreement, word order, and other purely syntactic details may be the focus of rules, but other models may additionally include considerations like lexical semantics. There are many different grammatical formalisms that rely on different syntactic theories, and the structures that are produced by parsing, or parses, can vary greatly between these formalisms. A phrase structure is an ordered, labeled tree that expresses hierarchical interactions among specific groupings of words called phrases [6]. It is one of the many formalisms that explain the syntactic analysis of a sentence. Dependency structure, which indicates binary grammatical relationships between words in a phrase, is another option for representation. There exist "shallow" representations of syntactic structures, in contrast to "deep" representations, where the maximum depth is strongly constrained. Finite state approaches are commonly used to create such representations.

Parse structures are primarily significant because of the grammatical information they provide to modules that carry out semantic, pragmatic, and discourse processing. This information is essential for tasks such as text summarization, question-answering, and machine translation. Parsing can be seen as a crucial element of traditional NLP systems, and the accuracy of the parses can greatly affect the overall effectiveness of an application.

A natural language grammar often allows for a wide range of parses for a given input sentence. This is because formal grammars often overlook important aspects of a language's structure, meaning, and usage, leading to numerous parses that people would not consider logical. By computing isolated portions of the parses and saving them in a table, significant practical issues in computation and storage can be avoided. This has the benefit of allowing multiple parses to utilize the same fragment. Tabular parsing is the correct term for this. Numerous tabular parsing techniques can compute and store exponentially many parses while only requiring polynomial time and space.

Probabilistic parsing, which depends on the attribution of probabilities to grammatical rules, is one special case of this. A parse's probability is calculated as the sum of the probabilities of the rules used to construct it. By selecting the parse with the highest likelihood, disambiguation is achieved. Contrary to approaches that rely on a deep understanding of linguistics for syntactic disambiguation, probabilistic parsing and weighted parsing are successful due to their adaptability and scalability.

Context-free grammar, or CFG, is a widely used formal method for representing constituent structure in natural language. Phrase-structure grammars are another name for context-free grammars, and Backus-Naur form, often referred to as BNF, is the formalization used. It wasn't until Chomsky that the concept of basing a language on constituent structure was formalized [6].

To the left of the arrow, each context-free rule has a single non-terminal symbol that denotes a cluster or generalization, and to the right, an ordered list of one or more terminals and non-terminals. The lexical category or part of speech for each word is connected to a non-terminal in the dictionary [6].

A context-free grammar (CFG) can be viewed in two different ways: as a mechanism for generating new sentences and as a means of assigning a specific structure to a sentence. We can interpret the arrow as meaning to "rewrite the symbol on the left with the string of symbols on the right" if we think of a context-free grammar as a generator [15].

The formal language, as defined by a CFG, consists of the collection of strings that can be derived from the selected start symbol. Each grammar must have a specific start symbol, commonly referred to as S . S is typically considered the "sentence" node because context-free grammars are often used to generate sentences. The other nodes are defined in **Table 4.1**. Grammatical sentences are those that can be produced from a grammar and are part of the formal language specified by that grammar. Ungrammatical sentences are those that cannot be generated by a specific formal grammar and do not belong to the language that the grammar defines. This is because context can often determine whether a sentence belongs to a specific natural language.

A lexicon consists of words and symbols, while a collection of rules or productions defines the different ways in which the symbols of a language can be combined and arranged. Together, these components form a context-free grammar. Rule-free context: we can combine the previous rules with others that describe details about the vocabulary specified by the four parameters T , N , R , and S because G can be hierarchically embedded:

$$G = \langle T, N, S, R \rangle. \quad (4.8)$$

Each of the parameters contains the following data:

- T is set of terminal symbols that corresponds to words in the language (lexicon);
- N is set of non-terminal symbols that express abstractions over the terminals (or variables);
- S is start symbol (one of the non-terminals);
- R is rules/productions of the form $X \rightarrow \gamma$, where X is a nonterminal and γ is a sequence of terminals and non-terminals (may be empty);
- A grammar G generates a language L .

As shown in the **Fig. 4.2**, h a given context-free grammar defines the rules for constructing valid sentences. Context-free grammar rules specify the relationships between different constituents, such as subjects, verbs, objects, and modifiers. The parsing process disambiguates such sentences and selects the most appropriate syntactic structure.

● **Table 4.1** Token label definitions of lexical parsing processes

Token Label	Description
ADJP	Adjective Phrase
ADVP	Adverb Phrase
CONJP	Conjunction Phrase
FRAG	Fragment
INTJ	Interjection
NAC	Not a constituent
NP	Noun Phrase
NX	Head subphrase of complex noun phrase
PP	Prepositional Phrase
QP	Quantifier Phrase
RRC	Reduced Relative Clause
S	Simple declarative clause (sentence)
SBAR	Clause introduced by complementizer
SBARQ	Question introduced by wh-word
SINV	Inverted declarative sentence
SQ	Inverted yes/no question
UCP	Unlike Co-ordinated Phrase
VP	Verb Phrase
WHADJP	Wh-adjective Phrase
WHADVP	Wh-adverb Phrase
WHNP	Wh-noun Phrase
WHPP	Wh-prepositional Phrase

The idea of derivation provides a language with its definition. If a set of rule applications can transform one string into another, then the first string derives the second. More precisely, derivation is a generalization of direct derivation, according to Hopcroft and Ullman [16].

Let $\alpha_1, \alpha_2, \dots, \alpha_m$ be strings in $(T \cup N)^*$, $m \geq 1$, such that α_1 derives α_m :

$$\alpha_1 \Rightarrow \alpha_2, \alpha_2 \Rightarrow \alpha_3, \dots, \alpha_{m-1} \Rightarrow \alpha_m. \quad (4.9)$$

The language L produced by a grammar G can thus be properly defined as the set of strings made up of terminal symbols that can be deduced from the prescribed start symbol S :

$$L_G = \{w \mid w \text{ is in } T^* \text{ and } S \text{ derives } w\}. \quad (4.10)$$

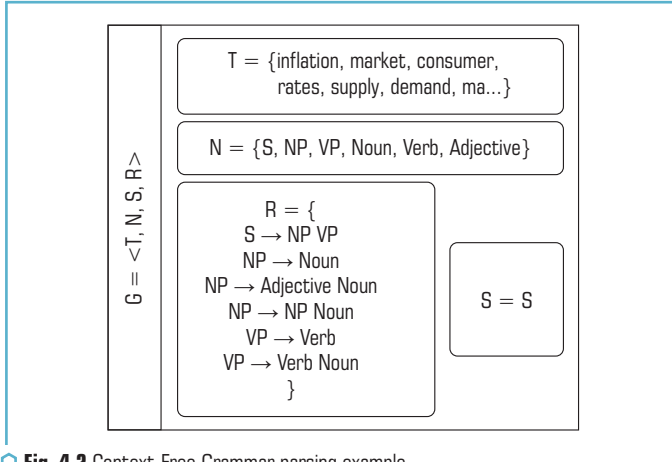


Fig. 4.2 Context-Free Grammar parsing example

A treebank is a corpus in which each sentence is tagged with a parse tree. In parsing, as well as in linguistic studies of syntactic issues, treebanks are crucial. The process of mapping a group of words to their parse tree is known as syntactic parsing.

Treebanks are generally made by parsing each sentence with a parse that is then hand-corrected by human linguists. As shown in the Fig. 4.3, the constituency parsing (parse tree) provides a hierarchical structure of the sentence, while the universal dependencies give a flatter representation of the syntactic relationships between words in the sentence. Both methods are used for syntactic analysis in natural language processing, with dependency parsing being more compact and favored for some tasks, while constituency parsing provides a hierarchical structure often used for deeper linguistic analysis.

<pre>(ROOT (S (NP (DT The) (JJ central) (NN bank)) (VP (VBD raised) (NP (NN interest) (NNS rates)) (S (VP (TO to) (VP (VB curb) (NP (NN inflation)))))) (...)) a</pre>	<pre>det(bank-3, The-1) amod(bank-3, central-2) nsubj(raised-4, bank-3) root(ROOT-0, raised-4) compound(rates-6, interest-5) obj(raised-4, rates-6) mark(verb-8, to-7) advcl(raised-4, verb-8) obj(verb-8, inflation-9) b</pre>
--	---

Fig. 4.3 Parsing type: *a* – constituency parsing (Parse tree); *b* – dependency parsing

It can be helpful to have a normal form for grammars when each production has a certain form. A context-free grammar, for instance, is in Chomsky normal form (CNF) [6] if it is not null and each production also has one of the following forms: $A \rightarrow BC$ or $A \rightarrow a$.

In other words, each rule has either two non-terminal symbols on the right side or one terminal sign. Binary branching, or having binary trees (down binary branching to the prelexical nodes), is a feature of Chomsky normal form grammars. A weakly equivalent Chomsky normal form grammar can be created from any context-free grammar. Chomsky adjunction is the production of a symbol A with a possibly infinite series of symbols B with a rule of the type $A \rightarrow AB$.

The context-free nature of our grammar rules gives rise to the advantage of dynamic programming. Once a constituent has been identified in a section of the input, we can record its presence and make it available for use in any subsequent derivation that might require it. This saves time and storage because subtrees can be looked up in a table instead of being reanalyzed. The Cocke-Kasami-Younger (CKY) algorithm, which is the most popular dynamic programming-based parsing method, is presented in this section. A comparable strategy is chart parsing [13, 16], and dynamic programming techniques are often referred to as chart parsing techniques with the requirement of being in CNF.

Any context-free grammar (CFG) can be transformed into Chomsky normal form (CNF) while still preserving the language, as long as it does not generate the empty string. Some definitions of CNF allow the symbol S as an admissible rule to account for the empty string, as long as S does not appear on the right-hand side of any rule. We'll use T to represent the table used in the CKY algorithm. The table's elements, or items as we'll call them, are represented by the notation $P[i, A, j]$, where $A \in N$ and $0 \leq i \leq j \leq n$, and n is the length of the input string $w = a_1 \dots a_n$. It is best to think of the numbers i and j as input positions: the position 0 comes before a_1 , the position i with $1 \leq i \leq n-1$, w separate the symbol placement a_{i-1} and a_i in w , and the position n comes after a_n .

The substring $a_{i+1} \dots a_j$ of w can be obtained from non-terminal A if an item $P[i, A, j]$ is added to the table. Considering that the algorithm's primary objective is to add item $P[0, S, n]$ to the table, this could be seen as a partial recognition outcome. Only when the input string is correct, will this item be discovered at the end of the process.

Fig. 4.4 shows the display of the algorithm.

The algorithm considers substrings that end in j for each input location and determines the non-terminals from which the substrings can be derived. The substrings a_j of least length are considered first, then the Chomsky normal form suggests that any parse of such a substring must contain a single instance of the rule in the form $A \rightarrow a_j$. After that, substrings $a_{i+1} \dots a_j$ of greater lengths ($j > i+1$) are taken into consideration. The CNF suggests that if such a substring can be derived from A , then there is a rule $A \rightarrow BC$ (some B and C), where $i < k < j$, and $a_{i+1} \dots a_k$ and $a_{k+1} \dots a_j$ to a_k and a_{k+1} to a_j can be derived, respectively, for some choice of k .

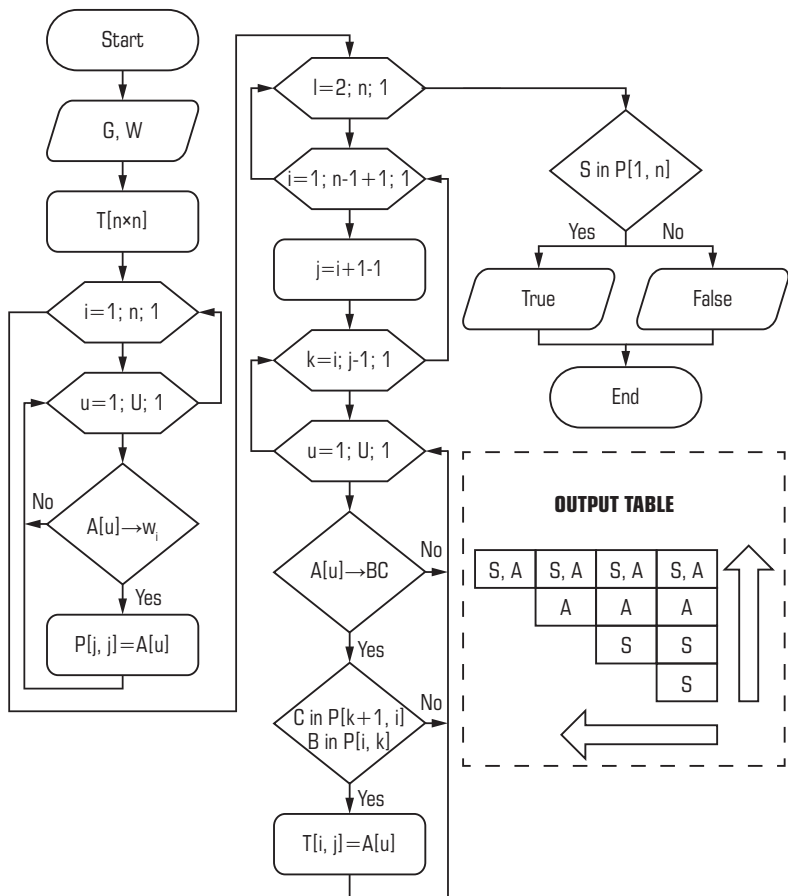


Fig. 4.4 The Cocke-Kasami-Younger (CKY) algorithm

4.3 DEVELOPING MODELS FOR SEMANTIC ROLE LABELING

The first step in any research project involving Natural Language Processing (NLP) classifiers is data collection. It is crucial to identify and gather relevant raw data sources [17]. These sources should encompass a wide range of materials, including financial news articles, annual reports, cyber incident reports, network traffic logs, and cybersecurity threat feeds.

Data collection. Financial news articles serve as a primary source of textual data for the economic aspect of the research. These articles are typically rich in content related to economic events, market dynamics, company performance, and economic indicators. To collect this data, we will consider various reputable financial news outlets and databases such as Bloomberg, Reuters, CNBC, and financial news sections of major newspapers. The selection of these sources will be based on their relevance, coverage, and the availability of structured and unstructured data. Annual reports of companies are another valuable source of economic data. These documents provide in-depth information about a company's financial performance, strategic goals, and risk assessments. The data will be collected from public sources, such as company websites, financial regulatory authorities like the U.S. Securities and Exchange Commission (SEC), and databases of publicly available annual reports. This data will be useful in understanding how companies describe their financial status and outlook, and how they frame economic information within their reports.

NLP systems require both correct and incorrect data for training and testing purposes. Obtaining correct data is relatively easy, but obtaining data with errors like typos and misspellings is challenging. Generating incorrect data can be a solution, but it is difficult to ensure that the generated texts correspond to real human mistakes. In this paper, the authors focused on collecting incorrect texts and misspellings from players through an automated web application. They used this data to build a model of common errors, which can be used to generate a large amount of authentic-looking erroneous texts [18].

The cybersecurity aspect of the research necessitates the collection of data related to cyber incidents. Cyber incident reports, often generated by Computer Emergency Response Teams (CERTs) and security organizations, contain valuable information about security breaches, attack vectors, and mitigation strategies. Sources for collecting cyber incident reports will include both government and private organizations, such as the United States Computer Emergency Readiness Team (US-CERT), the Center for Internet Security (CIS), and various industry-specific CERTs. These reports will provide insights into the language and semantics used to describe cyber threats and incidents. For a deeper understanding of the cybersecurity context, network traffic logs are an essential data source. These logs contain detailed information about network activities, including traffic patterns, protocols, and communication behaviors. Data collection in this category may involve partnerships with organizations that can provide anonymized network traffic data, or accessing publicly available datasets and network monitoring tools. These logs will help in analyzing the language and semantics used in network communications during cyber incidents. To keep up with the rapidly evolving cybersecurity landscape, cybersecurity threat feeds will be a valuable source of real-time data. These feeds provide information on emerging threats, vulnerabilities, and malicious activities. Sources for collecting threat feeds include government agencies, commercial threat intelligence providers, and open-source threat intelligence platforms. The data from these feeds will enable the analysis of the language and semantic roles used in describing emerging threats and vulnerabilities.

It is imperative to ensure that the collected data aligns with the specific research objectives of semantic role labeling and analysis [14]. The data will be chosen in such a way that it encompasses a broad spectrum of economic and cybersecurity language, including event descriptions, indicators, actors, and actions. The alignment will allow for meaningful analysis and classification of semantic roles in the data, furthering our understanding of the language used in these domains [18].

Data preprocessing. Data preprocessing is a crucial stage in NLP research, where we transform the collected raw data into a format that is suitable for analysis and classification [19]. Data cleaning is the initial step in the data preprocessing process. It involves the removal of any noise, irrelevant information, special characters, and inconsistencies present in the raw data. Financial news articles, annual reports, cyber incident reports, and other sources may contain various forms of noise, such as advertisements, metadata, HTML tags, and extraneous information not relevant to the research objectives [20]. Cleaning the data ensures that we are left with only the textual content that matters for our analysis.

Tokenization is the process of splitting the text into individual words or tokens. Tokens are the basic units of text that can be analyzed independently. By tokenizing the data, we break down the text into its constituent parts, making it amenable to further analysis. For example, the sentence "The stock market is volatile" would be tokenized into the tokens: ["the", "stock", "market", "is", "volatile"]. To ensure consistency in the data and prevent case sensitivity issues, all text is converted to lowercase [20]. Lowercasing ensures that words like "Economy" and "economy" are treated as the same word during analysis. This step helps in creating a uniform text corpus for analysis. Common words known as stopwords, such as "and", "the", "in", etc., do not carry significant meaning in the analysis and can be removed from the data to reduce noise and improve processing efficiency. However, it's important to note that in some cases, stopwords may be domain-specific and could carry relevant information. This aspect will be considered when removing stopwords, ensuring that domain-specific stopwords are retained if necessary [21].

Both economic and cybersecurity domains have their unique terminology, jargon, and linguistic patterns. It is crucial to adapt the preprocessing steps to accommodate these domain-specific characteristics. For example, in the economic context, financial terms such as "GDP", "dividends", and "NASDAQ" may need normalization, and currency symbols need to be handled consistently. In the cybersecurity domain, domain-specific jargon like "DDoS attack", "malware", and "firewall" should be treated in a manner that preserves their specific meanings. The data preprocessing pipeline involves a sequential application of the above steps. Once the raw data has been cleaned, tokenized, lowercased, and had stopwords removed, domain-specific preprocessing is applied to tailor the data for each respective context [21]. This pipeline ensures that the data is transformed into a structured, noise-free, and consistent format that can be used in subsequent stages of semantic role labeling and analysis.

Text annotation and Labeling. Text annotation is a fundamental step in NLP that involves marking specific elements of the text to identify and extract target semantic roles or entities. In the context of our research, we aim to identify and label semantic roles in both economic and cybersecurity domains. These roles will provide the foundation for further analysis and classification [22].

In the economic context, the identification of semantic roles is essential for understanding the relationships and interactions between various entities and actions. The following are some of the semantic roles that we will annotate and label in this domain:

1. Buyer: the entity or role responsible for purchasing goods or services.
2. Seller: the entity or role responsible for selling goods or services.
3. Investor: the entity or role involved in providing capital or funds for investment purposes.
4. Regulator: the entity or role responsible for enforcing rules and regulations within the economic domain.

These roles capture the key entities and actions involved in economic activities and transactions. Annotating and labeling them will enable to analyze how these roles are represented and the relationships between them in economic texts.

In the cybersecurity context, semantic role annotation is critical for understanding the dynamics of cyber incidents, threats, and vulnerabilities. The following are some of the semantic roles that we will annotate and label in this domain:

1. Attacker: the entity or role responsible for initiating a cyberattack.
2. Target: the entity or role that is the victim or the primary target of the cyberattack.
3. Exploit: the means or action used by the attacker to compromise a system or network.
4. Vulnerability: the weakness or flaw in a system or software that the attacker exploits.

These roles are central to understanding the various elements involved in cyber incidents and attacks [23]. Annotating and labeling these roles will enable to explore how these roles are depicted in cybersecurity-related texts and the relationships between them.

The annotation process involves manually identifying instances of the defined semantic roles in the preprocessed text. This process may involve using specialized annotation tools or guidelines tailored to the economic and cybersecurity domains. Annotators will mark text spans or assign labels to specific words or phrases that correspond to the roles identified. Understanding the relationships between the annotated roles is a critical aspect of this research. In both economic and cybersecurity contexts, the interactions and dependencies between roles can be complex. Analyzing these relationships will provide insights into the structure and semantics of the text data [22]. For instance, in economic texts, we may explore how buyers and sellers interact, or how regulators oversee financial transactions. In cybersecurity, we can investigate the interactions between attackers, targets, exploits, and vulnerabilities to gain a deeper understanding of cyber incidents.

Ensuring consistency in labeling is crucial to maintain the quality and reliability of the annotated data. Annotation guidelines and inter-annotator agreement assessments may be used to validate the consistency of role labeling, especially in cases where multiple annotators are involved.

Semantic Role Labeling. SRL is a key step that involves the identification and classification of semantic roles within the text. For our research, we will focus on economic and cybersecurity texts and employ appropriate SRL techniques to fulfill this objective.

Selecting the right SRL model is vital to the success of our research. Given the specific nature of our domains (economic and cybersecurity contexts), we must decide whether to use pre-trained SRL models, develop domain-specific models, or adopt a combination of both approaches:

- pre-trained models: pre-trained SRL models, such as those based on large-scale general corpora like OntoNotes or Universal Dependencies, can be a good starting point. They capture a broad range of semantic roles and syntactic structures in natural language, making them potentially useful for our analysis [24];
- domain-specific models: economic and cybersecurity texts often have unique terminologies and linguistic patterns. To address this, we may consider developing or fine-tuning domain-specific SRL models. These models can be trained on domain-specific datasets, making them more attuned to the intricacies of economic and cybersecurity texts [25].

The application of SRL techniques involves using the selected models to process the annotated data and extract semantic roles. Some common SRL methods that can be employed for this purpose include:

- dependency parsing: dependency parsing is a technique that analyzes the grammatical structure of a sentence. It identifies the relationships between words and assigns labels to these relationships. In the context of SRL, dependency parsing can be used to identify the roles that different words play in a sentence, such as identifying the subject, object, and other dependents of a verb [26];
- frame-based SRL: frame-based SRL is a method that involves identifying specific semantic frames, which are predefined structures that capture the relationships between roles and their associated arguments in a sentence. This method can be particularly useful for extracting domain-specific roles and their respective arguments in economic and cybersecurity texts [25].

Once the semantic roles have been identified, the next step is to classify them into their respective categories. In economic texts, this might involve classifying roles as "buyer", "seller", "investor", or "regulator". In cybersecurity texts, roles could be classified as "attacker", "target", "exploit", or "vulnerability". Role classification provides a structured representation of the roles in the text, making it easier to analyze and interpret the relationships between these roles.

To ensure the accuracy and quality of the SRL output, it is essential to evaluate the performance of the chosen SRL models. This evaluation can be done using standard metrics such as precision, recall, F1-score, and inter-annotator agreement. The evaluation process helps measure how well the SRL techniques are capturing the semantic roles within the text.

Model training and evaluation. After completing the Semantic Role Labeling (SRL) phase and obtaining annotated data, the focus shifts to the critical stages of model training and evaluation. Model training involves using the annotated data to train SRL models, considering choices such as pre-trained models, domain-specific models, or a combination of both [27]. The training process includes data preparation, model selection, feature engineering (for domain-specific models), training procedures, and leveraging transfer learning techniques to adapt knowledge from pre-trained models to the target domain [28].

Fine-tuning is a crucial step in the model development process. It involves making adjustments to the model's architecture and hyperparameters to ensure it performs optimally on the target task. In the context of economic and cybersecurity texts, fine-tuning may involve adapting the model to understand domain-specific terminology, syntax, and semantics [29]. This step helps the model capture nuances and nuances that are specific to the respective domains.

Model evaluation is essential to measure the performance of the trained and fine-tuned SRL models. It ensures that the models effectively extract semantic roles from economic and cybersecurity texts. The following metrics are commonly used for SRL model evaluation:

- F1 score: the F1 score is a balance between precision and recall and is particularly useful when there is an imbalance between classes. It provides a single score that summarizes the model's performance;
- precision: precision measures the ratio of correctly predicted positive instances to the total instances predicted as positive. In SRL, precision indicates how accurately the model labels semantic roles;
- recall: recall measures the ratio of correctly predicted positive instances to the actual positive instances. In SRL, recall indicates the model's ability to capture all instances of the semantic roles in the text;
- accuracy: accuracy measures the overall correctness of the model's predictions. It is the ratio of correctly predicted instances to the total instances.

To ensure consistent performance and generalizability, cross-validation techniques can be employed, involving the splitting of data into multiple subsets for robust model evaluation. Fine-tuning processes may also optimize hyperparameters, including learning rates, batch sizes, and regularization parameters, aiming to find the optimal configuration for the best model performance. These approaches collectively contribute to the development of effective SRL models tailored to the specific demands of economic and cybersecurity texts.

Feature engineering. Feature engineering involves the extraction of relevant features from the data, which can provide valuable linguistic information to improve the accuracy and effectiveness of the SRL models.

Linguistic features are fundamental to understanding and representing the structure and meaning of text. These features can include:

- part-of-speech (POS) tags: POS tags are labels assigned to each word in a sentence, indicating the word's grammatical category (e.g., noun, verb, adjective). Incorporating POS tags into the feature set can assist SRL models in understanding the syntactic roles of words in a sentence, which is crucial for identifying semantic roles [30];
- syntactic dependencies: syntactic features capture the grammatical relationships between words in a sentence. These dependencies help in understanding how words are connected in terms of subject-verb-object relationships, modifiers, and more. Syntactic dependency trees and labels can be used as features to provide additional context for semantic role identification [31];

– n-grams: n-grams are contiguous sequences of n words from a text. By including n-grams as features, we can capture the local context around a word or phrase, which is particularly useful in disambiguating word senses and identifying semantic roles [30];

– word embeddings: word embeddings, such as Word2Vec or GloVe, represent words as continuous vector spaces, where words with similar meanings are located close to each other. These embeddings can be used as features to provide semantic information, enabling the model to understand word similarity and context [32].

Actionable model creation. The creation of actionable models represents the culmination of the research efforts, where the semantic roles identified in economic and cybersecurity texts are translated into practical applications. These models have the potential to drive informed decisions, enhance security, and provide valuable insights in these domains. In the following chapters, we will explore the practical implementation and real-world impact of these actionable models.

In the economic context, actionable models can be created to support various applications, including:

– investment decisions: semantic roles like "buyer", "seller", and "investor" can be leveraged to inform investment decisions. By tracking the activities and sentiments associated with these roles in financial news articles, the model can provide insights into market trends, potential investment opportunities, or risks;

– sentiment analysis: analyzing the roles associated with sentiment-laden words and phrases in economic texts can enable sentiment analysis. This can help in understanding market sentiment, investor confidence, and public perception, which can be valuable for financial professionals and decision-makers [20];

– sentiment analysis: analyzing the roles associated with Predictive models can be developed by correlating semantic roles with financial indicators. For instance, identifying patterns in how buyers and sellers are described in news articles and their impact on stock prices can aid in market predictions;

– regulatory compliance: models can be created to identify regulatory violations or non-compliance by tracking the actions of regulators and the entities they oversee in annual reports and financial documents.

In the cybersecurity context, actionable models can be developed for a range of applications, such as:

– threat detection: by analyzing semantic roles like "attacker" and "exploit" in network logs and cybersecurity reports, actionable models can be built to detect and respond to security threats in real time;

– incident response: models can be used to identify the roles involved in cyber incidents, helping incident response teams understand the nature of the attack, its impact, and potential countermeasures;

– threat intelligence: by analyzing semantic roles, such as "vulnerability" and "target", actionable models can provide insights into emerging threats, vulnerabilities, and potential targets, assisting in proactive threat intelligence;

– security risk assessment: actionable models can assess security risks by monitoring the roles and actions associated with different entities in a network. This can help organizations identify weak points and vulnerabilities.

The development of actionable models has the potential to provide significant benefits in both economic and cybersecurity contexts. These models can enhance decision-making, improve security, and enable proactive responses to changing conditions and threats.

Real world testing. Real-world testing is a crucial phase, as it allows us to assess how well the models work in practical, dynamic settings.

Real-world testing involves applying the actionable models to different scenarios and assessing their performance and usability [33]. These scenarios may include:

- economic analysis: testing the model's ability to provide investment recommendations or sentiment analysis in real-time as new financial data becomes available;
- cybersecurity defense: assessing the model's effectiveness in real-time threat detection and incident response within a live network environment;
- predictive capabilities: evaluating the model's predictive capabilities by monitoring its performance over an extended period to gauge its long-term accuracy;
- usability in practical tasks: testing the model's utility in practical cybersecurity tasks, such as security risk assessment, threat intelligence, and regulatory compliance monitoring.

Assessing model performance involves monitoring how well the actionable model performs in real-time. Key metrics and indicators should be observed, such as:

- accuracy: how well the model's predictions match real-world outcomes;
- precision and recall: the model's ability to correctly identify and act upon semantic roles in dynamic situations;
- latency: the time it takes for the model to process data and provide actionable insights.

The real-world testing phase provides an opportunity to evaluate the model's adaptability and scalability. Can it accommodate new data sources, handle unexpected scenarios, and scale to meet the demands of practical applications? These aspects are critical for assessing the model's long-term usability. Real-world testing often uncovers areas for improvement. Gathering feedback from users and stakeholders involved in the practical application of the model is invaluable. This feedback can guide iterative refinements and updates to enhance the model's performance and utility.

Usability testing focuses on how well the actionable model fits into the workflow of users. Is it user-friendly, easy to integrate, and does it meet the specific needs of the users in economic or cybersecurity roles? Real-world testing is the ultimate litmus test for the actionable models developed in our research. It's where the rubber meets the road, and the effectiveness of these models in practical economic and cybersecurity scenarios is demonstrated. The insights gained from this phase will provide valuable feedback for further refinement and real-world deployment, ultimately contributing to the real-world application of semantic role labeling and analysis. In the final chapters, we will explore the broader implications and contributions of our research in these critical domains.

Iterative refinement. While we have developed actionable models that are ready for real-world testing and deployment, it is important to focus on the importance of continuous refinement and adaptation. In dynamic domains, staying current and responsive to changes in linguistic patterns and domain-specific developments is essential.

The worlds of economics and cybersecurity are in a state of constant evolution. New terminologies, trends, and linguistic patterns emerge regularly. As a result, actionable models must be continuously refined to stay relevant and effective [20]. The need for iterative refinement is driven by several factors:

- dynamic language use: language use evolves over time, and new terms and phrases enter the lexicon. Iterative refinement allows models to adapt to these linguistic changes and remain accurate in their predictions [34];
- understanding machine learning: from theory to algorithms [30];
- changing threat landscape: in cybersecurity, the threat landscape is constantly changing as attackers develop new tactics and exploit novel vulnerabilities. Models must be updated to detect these emerging threats effectively;
- market dynamics: economic markets are influenced by various factors, including geopolitical events, economic policies, and global trends. Refinement is necessary to capture how these changes affect economic roles and actions;
- user feedback: feedback from users of the actionable models provides valuable insights into areas where improvement is needed. Iterative refinement is a response to this feedback.

Iterative refinement also involves adapting to domain-specific developments in economics and cybersecurity. Some ways to achieve this include:

- regular data updates: regularly updating the training data with the latest economic reports, financial news, cybersecurity incidents, and threat reports to ensure that the model reflects the current state of the domain;
- domain expertise: involving domain experts who can provide insights into the evolving landscape and guide model adjustments to account for new trends and terminologies;
- model re-training: re-training the model using up-to-date data and fine-tuning it to account for changes in the domain;
- incorporating external knowledge sources: integrating external sources of domain knowledge, such as industry reports or expert opinions, to inform model adjustments.

User feedback is a central component of iterative refinement [34]. Ensuring that the actionable models align with the needs and expectations of users is paramount. This may involve:

- user surveys and interviews: conducting surveys or interviews with users to gather their input on model performance, usability, and areas for improvement;
- user training: offering training sessions to users to familiarize them with the model and gather insights into how it can better fit into their workflow;
- user-driven feature requests: encouraging users to suggest new features or modifications that would enhance the model's usability [34].

Iterative refinement is an ongoing process, and continuous evaluation is crucial to assess the effectiveness of model updates. This evaluation should include the monitoring of key metrics, usability testing, and the measurement of model performance in real-world scenarios.

Deployment and practical use. The ultimate goal is to ensure that the model is capable of providing valuable insights and supports decision-making processes in these domains.

The deployment of actionable models in real-world contexts involves several considerations, including:

- infrastructure and scalability: ensuring that the necessary computational infrastructure is in place to support the model's real-time processing needs and scalability to handle increasing data volumes;
- data integration: integrating the model with data sources, ensuring that it can access relevant economic and cybersecurity texts or data feeds;
- user training: providing training and onboarding for users who will interact with the model to ensure they understand how to utilize it effectively;
- security and compliance: ensuring that the deployment adheres to security standards and regulatory compliance, especially in the cybersecurity domain where sensitive information is involved.

For practical use, the model should be designed to facilitate user interaction and interpretation of results. This may include creating user-friendly interfaces, dashboards, or reports that allow users to make informed decisions based on the insights provided by the model. Deployment is not the endpoint but rather the beginning of an ongoing cycle of monitoring and continuous improvement. Regularly evaluating the model's performance, gathering user feedback, and making necessary refinements is essential to ensure that the actionable model remains effective in the long term.

4.4 METHODOLOGICAL FOUNDATIONS FOR DEVELOPING A SEMANTIC ROLE CLASSIFIER FOR CYBER THREAT ANALYSIS AND ECONOMICAL SPHERE USING ARTIFICIAL NEURAL NETWORKS

ANNs have been applied in the study of language in various ways. The multi-layered perceptron (MLP) is the most practical ANN architecture for statistical modeling. MLPs have been expanded to represent both sequential and structured data and can be utilized for feature induction and probability estimation. Language modeling and parsing have been their most effective uses in NLP. MLPs can be reinterpreted as approximate versions of latent variable models, and they have served as an inspiration for much of the recent research in machine learning techniques.

Artificial neural networks, or simply "neural networks", are a general term for a group of computational models that have some characteristics in common with the networks of neurons present in the brain. They are often built to be educated using data and comprise of a distributed network of simple processing units. These were some of the earliest machine learning techniques in the field of artificial intelligence (AI), and they have had a significant impact on various areas of machine learning research. The majority of ANN research within AI no longer has any neurological underpinnings and is now mostly driven by engineering concerns [34]. Research in NLP has been primarily driven by its applicability for engineering solutions.

Unsupervised representation induction during learning is another characteristic that is frequently associated with ANNs. Some of the artificial neural networks (ANN) processing units do not have predefined meanings; instead, they develop them during training. In other instances, such as the unsupervised clustering of self-organizing maps, these units serve as the output of the

artificial neural network (ANN). In other instances, these units serve as an intermediary representation between the input and output of the ANN. These units are known as "hidden units"; they are comparable to latent variables. The multilayer perceptron (MLP) and its recurrent variations have been the most frequently used types of artificial neural networks (ANNs). MLPs are used for sequence modeling, categorization, and function approximation.

Another trait that is usually linked to ANNs is unsupervised representation induction during learning. Some of the processing units of an artificial neural network (ANN) gain their meanings during training rather than having them predefined. These units are used as the artificial neural network (ANN) output in other situations, such as the unsupervised clustering of self-organizing maps [24]. In other cases, these units act as a representational bridge between the ANN's input and output. They are referred to as "hidden units" and are similar to latent variables. The most popular varieties of artificial neural networks (ANNs) have been the multilayer perceptron (MLP) and its recurrent versions. Sequence modeling, categorization, and function approximation are all performed using MLPs.

In response to the argument that the perceptron algorithm could only learn a very small class of problems, multi-layered perceptrons (MLPs) were created as it is possible to see in **Fig. 4.5**. The perceptron algorithm learns to distinguish between output classes based on a linear combination of its input features. Because of its linearity, a perceptron can only solve problems that can be divided into classes of outputs by a line (or, more generally, a hyperplane) that can be drawn in the input space. The XOR function is a clear example of a problem that cannot be linearly separated because there is no line that can divide the zero cases (0, 0, 1, 1) from the one cases (0, 1, 1, 0) [35].

The input layer consists of neurons (also called nodes) that represent the features or input data for your problem. Each neuron corresponds to a specific feature, and these neurons pass their values to the neurons in the first hidden layer. An MLP can have one or more hidden layers, each consisting of multiple neurons. The number of hidden layers and the number of neurons in each layer are hyperparameters that can be adjusted based on the complexity of the problem. Each connection between two neurons (either between the input and hidden layers or between hidden layers) has an associated weight. These weights are the parameters that the network learns during training. The weights determine the strength of the connection and play a crucial role in shaping the network's behavior. Activation functions are applied to the weighted sum of inputs at each neuron to introduce non-linearity into the network. Each neuron in the hidden and output layers typically has an associated bias term. The bias allows the network to model shifts in the data that are not accounted for by the weights and is added to the weighted sum of inputs before the activation function is applied.

The middle layers of MLPs contain processing units whose outputs are a continuous non-linear function of their inputs. This addresses the restriction by incorporating multiple layers of units. An MLP can transform the input space into a new set of features, where the output classes become linearly separable due to the presence of these middle layers, also referred to as hidden layers. In reality, MLPs can approximate any arbitrary function due to the non-linearity of

the hidden units [34]. Backpropagation is a straightforward learning procedure for MLPs because the hidden unit functions are continuous [34].

The output of each neuron in a hidden layer is determined by the weighted sum of its inputs, including the bias term, passed through the activation function. This output is then used as input to neurons in subsequent layers. The output layer consists of neurons that provide the final output of the network. The number of neurons in this layer depends on the specific problem you are trying to solve. For classification tasks, you might have one neuron per class for softmax classification, while for regression tasks, there might be a single output neuron. The loss function measures the difference between the network's predictions and the true target values. The choice of the loss function depends on the type of problem, e.g., mean squared error for regression or cross-entropy for classification.

During training, the network adjusts its weights and biases to minimize the loss function. This is typically done using optimization algorithms like stochastic gradient descent (SGD) or its variants. Backpropagation is a key technique for computing gradients and updating the weights. To prevent overfitting, techniques like dropout, weight decay (L1 or L2 regularization), and early stopping can be employed to make the network generalize better to unseen data. An MLP with multiple hidden layers and appropriate activation functions can approximate complex functions and is widely used in various machine learning tasks. The design of the network, including the number of layers, neurons per layer, activation functions, and other hyperparameters, is highly dependent on the specific problem being addressed.

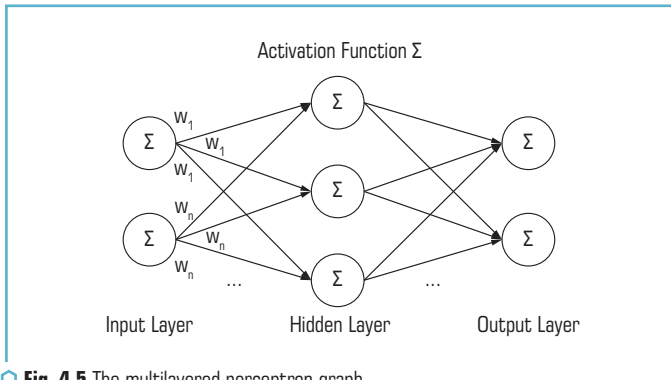


Fig. 4.5 The multilayered perceptron graph

The pursuit of understanding and representing words in a manner that accurately captures their semantic and syntactic connections has been a fundamental focus of research in Natural Language Processing (NLP). We came across word vectors during our journey, and they have revolutionized NLP applications. To grasp the fundamental principles of word embeddings, it is essential to comprehend the connection between word vectors, artificial neural networks, and the multi-layered perceptron (MLP).

Words in a continuous vector space are represented numerically as word vectors, also referred to as word embeddings. These embeddings provide syntactic and semantic connections between words, enabling natural language processing (NLP) systems to comprehend meaning and context. These compact numerical representations of words have opened new opportunities for tasks such as sentiment analysis, machine translation, and document classification. At the heart of this revolution lies the interaction between artificial neural networks and multi-layered perceptrons, which collaborate to capture word semantics and predict their context.

Word2Vec and FastText are two well-known models that have dominated the development of word vectors (Fig. 4.6). Both of these models train and generate word embeddings using artificial neural networks, specifically the multi-layer perceptron. The Word2Vec model for word embeddings was first presented by Mikolov. The Continuous Bag of Words (CBOW) and Skip-gram architectures are the two main architectures used by Word2Vec. Continuous Bag of Words (CBOW) predicts the target word by using the words in its context. The goal is to increase the likelihood of the target word given the context using a shallow neural network with one hidden layer. On the other hand, skip-gram guesses context words from a target word. Similar to CBOW, but with the aim reversed. In both situations, the word vectors are adjusted to capture linguistic correlations after the training process has fine-tuned the neural network weights [36].

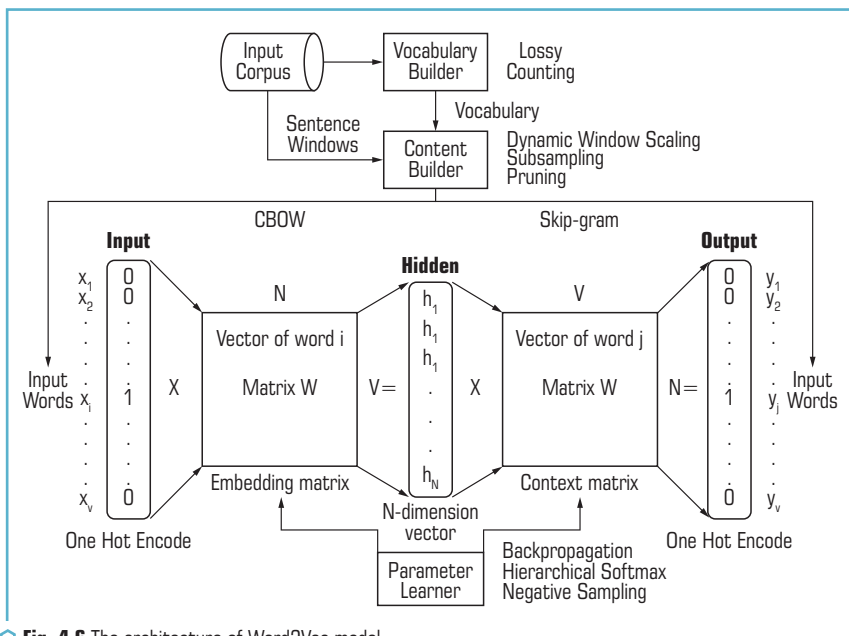


Fig. 4.6 The architecture of Word2Vec model

With a predefined vocabulary and a substantial text dataset as an initial input, Word2Vec can commence text processing. Although the vocabulary is typically broad, it can be condensed to include only common words. As depicted in **Fig. 4.7**, each word in the dictionary is assigned a vector representation using Word2Vec. Using a distributional similarity objective, Word2Vec aims to learn word vectors from a text corpus. Predicting which words will appear in the context of other words is necessary for this challenge. Operationally, Word2Vec utilizes the concepts of context words (O) and center words (C). While context words are the terms that appear around the center word in the text, center words are the words that are being considered.

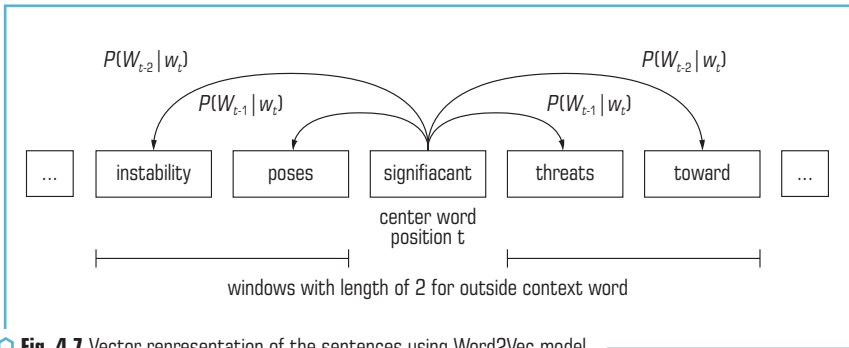


Fig. 4.7 Vector representation of the sentences using Word2Vec model

With a predefined Word2Vec uses the current word vectors to calculate the probability of a context word occurring, given the center word, based on the model. The goal is to adjust the word vectors to maximize the probability assigned to words that actually occur in the context of the center word. This adjustment is performed iteratively as the model processes the text. The central component of Word2Vec is the objective function, which is a cost or loss function that requires optimization. The objective function aims to maximize the likelihood of the context words surrounding the center words. and a substantial text dataset as an initial input, Word2Vec can commence text processing. Although the vocabulary is typically broad, it can be condensed to include only common words. Each word in the dictionary is assigned a vector representation using Word2Vec. Using a distributional similarity objective, Word2Vec aims to learn word vectors from a text corpus. Predicting which words will appear in the context of other words is necessary for this challenge. Operationally, Word2Vec utilizes the concepts of context words (O) and center words (C). While context words are the terms that appear around the center word in the text, center words are the words that are being considered [37].

The likelihood is formally defined as the product of the probabilities of predicting context words for each center word. However, for the sake of computational simplicity, Word2Vec converts products into sums and utilizes log likelihood instead. Word2Vec works with the average log likelihood. The sum of log likelihoods is divided by the number of words in the corpus. Word2Vec employs

a minimization objective function (denoted as $J(\theta)$) rather than maximizing it. By minimizing this objective function, the model aims to maximize its predictive accuracy:

$$L(\theta) \prod_{t=1}^T \prod_{\substack{-m \leq j \leq m \\ j \neq 0}} P(w_{t+1} | w_t; \theta); \tag{4.11}$$

$$J(\theta) = -\frac{1}{T} \log L(\theta) = -\frac{1}{T} \sum_{t=1}^T \sum_{\substack{-m \leq j \leq m \\ j \neq 0}} \log P(w_{t+1} | w_t; \theta). \tag{4.12}$$

Each word in the lexicon has a vector representation thanks to Word2Vec. The context and meaning of words are captured by these vectors.

Each word is associated with two-word vectors: one for its use as the center word and another for its use as a context word. The mathematical calculations and optimization procedure are made easier by this method. Although it could appear a little strange, it is a sensible decision that will help with word vector creation.

Word2Vec uses a specific equation to determine the likelihood of a context word arising given the center word. The description refers to "the expression in the middle bottom of my slide", indicating that the precise equation is shown visually rather than in the text [37]. However, the exact equation is not provided in the text:

$$P(p | c) = \frac{\exp(u_0^T v_c)}{\sum_{w \in V} \exp(u_w^T v_c)}. \tag{4.13}$$

By adding the vector representations of the two words, $U(O)$ and $V(C)$, the probability of a context word (O) occurring given a center word (C) is calculated. The dot product compares the similarity between the vectors representing the letters "o" and "c". A larger dot product indicates a higher degree of similarity and a greater likelihood. Exponentiation transforms everything into positive values, while probability distribution is created by normalizing the entire lexicon through summation. Similarity is indicated by positive values, while dissimilarity is indicated by negative numbers.

The softmax function is used to transform these dot product values into a probability distribution. The dot product is transformed by the softmax function, which guarantees that all values are positive. The outcome is then normalized to create a probability distribution. More related terms are given higher odds in this distribution.

The objective is to minimize the average negative logarithm probability of the model's predictions, or the objective function (J of theta). Optimizing the model's parameters, which in the case of Word2Vec are the word vectors, is necessary to minimize this function. Two vectors – the context vector and the center vector – are included in the parameters for each word:

$$R^n \rightarrow (0,1)^n, \text{ soft max}(x_i) = \frac{\exp(x_i)}{\sum_{j=1}^n \exp(x_j)} = p_i. \tag{4.14}$$

Calculus is used to modify the word vectors and reduce the loss function. The gradients, which indicate the direction of the steepest descent, are computed by the model. The word vectors are iteratively updated using these gradients in gradient descent algorithms to improve their ability to anticipate context words. The text explains how to utilize the chain rule to unravel intricate expressions and simplifies the process of calculating derivatives by dividing it into multiple steps.

An expectation, which is an average across all the context vectors weighted by their probabilities, is the result of the derivative calculation. The derivative in softmax-style models is calculated by subtracting the expected value from the observed value. If the model predicts word vectors that are similar to the observed context words, it is considered effective:

$$\theta^{new} = \theta^{old} - \alpha \Delta_{\theta} J(\theta). \quad (4.15)$$

There are various approaches to visualizing word vectors. One common approach is to utilize dimensionality reduction techniques, such as t-SNE, to project the high-dimensional word vectors into a lower-dimensional space that is more easily visualized [38]. This enables the exploration of clusters and patterns within the word vector space. Another approach involves visualizing word vectors in a semantic space, where words with similar meanings are positioned close to each other. This can be achieved by plotting the word vectors on a semantic map or by employing interactive visualization tools [38]. These visualizations aid researchers and practitioners in understanding the semantic relationships between words and exploring the structure of the word vector space. In addition to visualizing word vectors, there are methods available for enriching word vectors with subword information. By considering subword units, such as character n-grams, in addition to whole words, the word vectors can capture more detailed information about word morphology and compositionality. This is particularly useful for languages with rich morphology or for tasks that require an understanding of word formation and derivation. Furthermore, word vectors can be adapted and fine-tuned using various techniques. For instance, one study proposed adapting word vectors using a tree structure to incorporate visual semantics [39]. By combining visual features with word vectors, the resulting representations can capture both the visual and semantic aspects of words. This can be advantageous for tasks such as image captioning or visual question answering.

Tools and Software. For this research, we utilized the GloVe (Global Vectors for Word Representation) pre-trained Word2Vec model. The selected dataset, glove.6B.100d.word2vec, has a vector dimensionality of 100 and includes a large vocabulary size. To process and analyze the data, we utilized well-known Natural Language Processing (NLP) libraries. These included NLTK for tokenization and stemming, Gensim for integrating the Word2Vec model, and scikit-learn for constructing and training the classifiers. The machine learning framework used in this study was scikit-learn, which is a robust and versatile library for machine learning tasks. Deep learning techniques were implemented using the Keras library.

Hardware. Our experiments were conducted on a machine with an Intel Core i7 processor, 16 GB of RAM, and SSD storage. As well as on a high-performance computing cluster equipped with multiple CPUs, a dedicated GPU, ample RAM, and ample storage. This infrastructure facilitated the efficient processing of the large-scale dataset and the training of complex neural network architectures.

Data. The dataset used in this research comprises economic and cybersecurity text data collected from reputable sources, such as financial reports, research papers, and cybersecurity incident reports. The dataset is extensive, containing a diverse range of texts, which enables a comprehensive analysis of semantic roles in various contexts.

Preprocessing. Prior to analysis, the data underwent rigorous preprocessing steps. This involved tokenization, which breaks down the text into individual words, stemming to reduce words to their root forms, and domain-specific transformations to enhance the relevance of the data in economic and cybersecurity contexts.

Feature extraction. Word2Vec embeddings were used to convert words into numerical vectors. The Word2Vec model used a window size of 5 and employed negative sampling to generate precise word representations. These embeddings served as crucial features for subsequent semantic role labeling and analysis tasks.

Neural Network Architecture. Word2vec uses neural networks for training. TWord2vec uses neural networks for training. The following layers are presented:

- as many neurons as there are words in the training vocabulary make up one input layer;
- the dimensionality of the generated word vectors determines the size of the hidden layer, which is the second layer, in terms of neurons;
- the output layer, which has the same number of neurons as the input layer, is the third and final layer.

One-Hot Encoding is the simplest method of converting words into vectors. The size of this vector is determined by the number of words in the vocabulary, and each word has its own vector. The word representing itself is encoded at position 1, and all additional locations are encoded at position 0. The input layer receives the one-hot encoding of the center word. We train our neural network by randomly initializing the weights. Here, the neural network updates its weights using the backpropagation approach. The central word receives our input and produces a specific outcome. The softmax classifier is processing the output. Because the softmax classifier can convert the output into a probability, it is utilized. This vector indicates which terms in the lexicon are most likely to be associated with the input word.

Every time a relevant word's one-hot encoding is inputted, the weights between the hidden and output layers and the input layer are adjusted to ensure that the output corresponds to the paired word. The weights are adjusted based on the calculated difference between the current output and the predicted input. The vectors we need to locate are the weights between the input layer and the hidden layer. The fact that each of these words has a context and association makes them significant. Words with similar vectors or closer spacing are used in the same context.

Input parameters. The input parameters for the neural network included the Word2Vec embeddings that represented the words in the text data. These embeddings, combined with additional domain-specific features, provide comprehensive input for the semantic role labeling classifier, ensuring a nuanced analysis of the text.

Training and Evaluation. The LSTM network was trained using the Adam optimizer with a suitable learning rate. The dataset was divided into training, validation, and test sets to facilitate model

training and evaluation. Performance was assessed using evaluation metrics such as F1-score, accuracy, precision, and recall, providing a comprehensive view of the classifier's effectiveness in capturing semantic roles in economic and cybersecurity texts.

Limitations and Assumptions. Several limitations were identified during the research, including potential biases in the data sources and the inherent limitations of the Word2Vec model in capturing highly nuanced semantic relationships. Additionally, assumptions were made regarding the relevance and accuracy of the selected features, recognizing the necessity for additional research to improve the model and overcome these limitations.

Output Data. The analysis yielded valuable insights into the semantic roles present in economic and cybersecurity texts. The output data includes detailed semantic role annotations, which highlight key relationships within the texts. Visualizations and graphs were generated to present the findings, providing a clear and concise representation of the semantic structures in the analyzed texts (**Fig. 4.8**). Additionally, the research provided valuable implications for economic analysts and cybersecurity experts, enabling them to enhance their understanding of textual data in their respective fields.

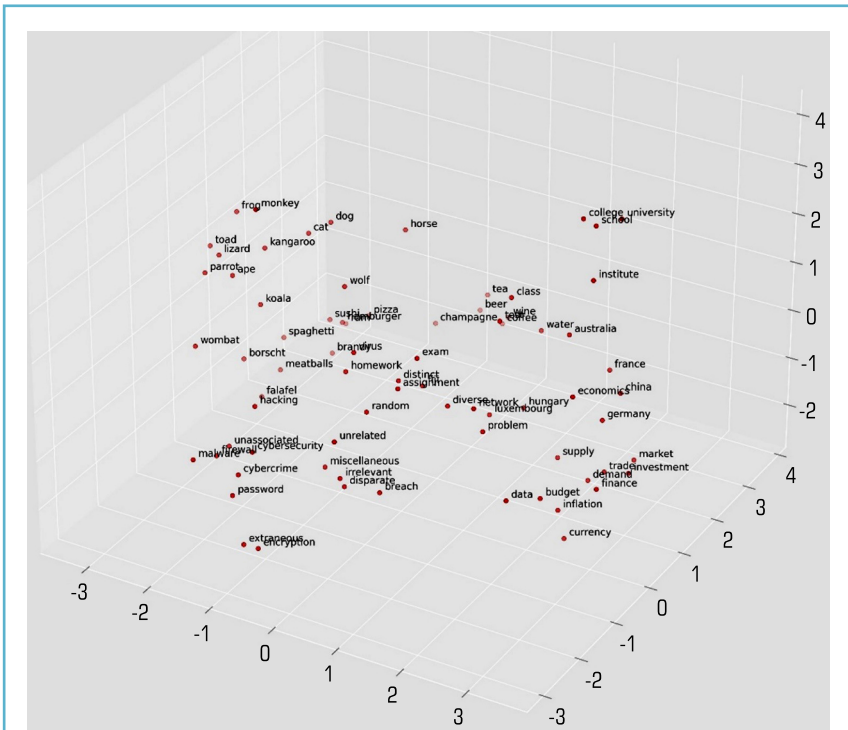


Fig. 4.8 Visualization of economical, cybersecurity and other non-connected words clustering

The three-dimensional PCA (Principal Component Analysis) visualization of words from diverse categories, including economic, cybersecurity, and non-connected words, provides valuable insights into the semantic relationships and similarities among these words. Through clustering, words within the same domain tend to group together, indicating their semantic proximity. Economic terms, such as "economics", "market", and "investment", form a distinct cluster, while cybersecurity-related words like "cybersecurity", "hacking", and "firewall" create another cohesive cluster. Non-connected words appear scattered, highlighting their lack of semantic correlation.

The clustered words can be leveraged for textual analysis tasks. Understanding the semantic context of words within specific domains can aid in sentiment analysis, topic modeling, and document classification, especially in economic and cybersecurity-related texts. Semantic clustering can enhance content recommendation systems. By identifying related terms, businesses can recommend relevant articles, research papers, or products to users based on their interests in economics or cybersecurity. The identified semantic relationships can contribute to constructing knowledge graphs, connecting economic concepts, cybersecurity terms, and other domains. This interconnected knowledge can be valuable for educational purposes or data-driven decision-making.

CONCLUSIONS

Semantic role labeling (SRL) plays a critical role in extracting important information from text, particularly in the fields of cybersecurity and economics. When it comes to interpreting financial reports, news stories, and economic literature, SRL is crucial. It assists in identifying important actors, events, and objects, which ultimately enhances decision-making and market analysis. This emphasizes the usefulness of deriving meaningful insights from textual data. In the field of cybersecurity, SRL (Semantic Role Labeling) is essential for understanding and processing text data that is related to security. It automates the analysis of large volumes of text, enabling faster responses to security concerns. In order to organize unstructured text data, evaluate risks, and make informed decisions in response to evolving security issues, NLP classifiers and machine learning models utilize SRL (Semantic Role Labeling).

The visualization provides a snapshot of word relationships but lacks contextual depth. Understanding the nuances of word meanings within sentences and paragraphs is crucial for conducting more precise semantic analysis. The quality and bias of the underlying data used to train the Word2Vec model can impact the clustering results. Biased data may result in distorted word representations, which can impact the accuracy of semantic relationships. Future research can explore advanced word embedding models, such as contextual embeddings (e.g., BERT), that capture word meanings based on surrounding context. These models provide more nuanced semantic representations, which can enhance the accuracy of clustering. Integrating textual data with other modalities, such as images, audio, or video, can enhance semantic analysis. Multimodal approaches enable a more comprehensive understanding of concepts, particularly in domains where visual or auditory cues play a significant role.

Overall, the findings suggest that self-regulated learning (SRL) can play a vital role in economic analysis and cybersecurity risk management. By accurately identifying and classifying semantic roles, NLP classifiers can facilitate the extraction of valuable information from textual data, thereby enabling more informed decision-making processes in economic contexts. In the cybersecurity domain, Security Risk Management (SRL) can aid in the detection and prevention of cyber threats, thereby enhancing the overall security posture of organizations and critical infrastructure. Future research can explore advanced word embedding models, such as contextual embeddings (e.g., BERT), which capture word meanings based on surrounding context. These models provide more nuanced semantic representations and can improve the accuracy of clustering.

However, further research is needed to address the challenges associated with SRL, such as the scarcity of annotated data for specific economic and cybersecurity domains. Additionally, the development of more robust natural language processing (NLP) classifiers and the integration of semantic role labeling (SRL) with other NLP techniques hold promise for advancing the application of SRL in these contexts. It highlights the potential of SRL in improving economic analysis and enhancing cybersecurity measures. by utilizing NLP techniques to extract valuable insights from textual data and mitigate risks in these domains. Future research should focus on addressing the challenges and further advancing the application of self-regulated learning (SRL) in economic and cybersecurity contexts.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Täckström, O., Ganchev, K., Das, D. (2015). Efficient Inference and Structured Learning for Semantic Role Labeling. *Transactions of the Association for Computational Linguistics*, 3, 29–41. doi: https://doi.org/10.1162/tacl_a_00120
2. Márquez, L., Carreras, X., Litkowski, K. C., Stevenson, S. (2008). Semantic Role Labeling: An Introduction to the Special Issue. *Computational Linguistics*, 34 (2), 145–159. doi: <https://doi.org/10.1162/coli.2008.34.2.145>
3. Lang, J., Lapata, M. (2014). Similarity-Driven Semantic Role Induction via Graph Partitioning. *Computational Linguistics*, 40 (3), 633–669. doi: https://doi.org/10.1162/coli_a_00195
4. Lample, G., Ballesteros, M., Subramanian, S., Kawakami, K., Dyer, C. (2016). Neural Architectures for Named Entity Recognition. *Proceedings of the 2016 Conference of the North*

- American Chapter of the Association for Computational Linguistics: Human Language Technologies. doi: <https://doi.org/10.18653/v1/n16-1030>
5. Manning, C., Schütze, H. (1999). Foundations of statistical natural language processing. MIT press.
 6. Chomsky, N. (1964). Aspects of the theory of syntax. doi: <https://doi.org/10.21236/ad0616323>
 7. Laukaitis, A., Ostasius, E., Plikynas, D. (2021). Deep Semantic Parsing with Upper Ontologies. Applied Sciences, 11 (20), 9423. doi: <https://doi.org/10.3390/app11209423>
 8. Cherifi, H. (2019). The Essential Contributions of Corpora in Language Research. NETSOL: New Trends in Social and Liberal Sciences, 4 (2), 62–73. doi: <https://doi.org/10.24819/netsol2019.08>
 9. Dupre, G. (2021). Empiricism, syntax, and ontogeny. Philosophical Psychology, 34 (7), 1011–1046. doi: <https://doi.org/10.1080/09515089.2021.1937591>
 10. Bolt, J., Coecke, B., Genovese, F., Lewis, M., Marsden, D., Piedeleu, R. (2019). Interacting conceptual spaces i: grammatical composition of concepts. Conceptual Spaces: Elaborations and Applications, 151–181. doi: https://doi.org/10.1007/978-3-030-12800-5_9
 11. Hare, A., Chen, Y., Liu, Y., Liu, Z., Brinton, C. G. (2020). On Extending NLP Techniques from the Categorical to the Latent Space: KL Divergence, Zipf's Law, and Similarity Search. doi: <https://doi.org/10.48550/arxiv.2012.01941>
 12. Jurafsky, D., Martin, J. H. (2018). Speech and language processing. Prentice Hall.
 13. Clark, A., Lappin, S.; Clark, A., Fox, C., Lappin, S. (Eds.) (2010). Unsupervised Learning and Grammar Induction. The Handbook of Computational Linguistics and Natural Language Processing, 197–220. doi: <https://doi.org/10.1002/9781444324044.ch8>
 14. Corral, Á., Boleda, G., Ferrer-i-Cancho, R. (2015). Zipf's Law for Word Frequencies: Word Forms versus Lemmas in Long Texts. PLOS ONE, 10 (7), e0129031. doi: <https://doi.org/10.1371/journal.pone.0129031>
 15. Goldsmith, J., van Riemsdijk, H., Williams, E. (1989). Introduction to the Theory of Grammar. Language, 65 (1), 150. doi: <https://doi.org/10.2307/414851>
 16. Hopcroft, J. E., Motwani, R., Ullman, J. D. (2001). Introduction to automata theory, languages, and computation, 2nd edition. ACM SIGACT News, 32 (1), 60–65. doi: <https://doi.org/10.1145/568438.568455>
 17. Zeroual, I., Lakhouaja, A. (2018). Data science in light of natural language processing: An overview. Procedia Computer Science, 127, 82–91. doi: <https://doi.org/10.1016/j.procs.2018.01.101>
 18. Hrkút, P., Toth, Š., Ďuračik, M., Meško, M., Kršák, E., Mikušová, M. (2020). Data Collection for Natural Language Processing Systems. Intelligent Information and Database Systems, 60–70. doi: https://doi.org/10.1007/978-981-15-3380-8_6
 19. Manning, C. D. (2009). An introduction to information retrieval. Cambridge university press.
 20. Pang, B., Lee, L. (2008). Opinion Mining and Sentiment Analysis. Foundations and Trends® in Information Retrieval, 2 (1-2), 1–135. doi: <https://doi.org/10.1561/1500000011>

21. Brown, P. F., Della Pietra, S. A., Della Pietra, V. J., Mercer, R. L. (1993). The mathematics of statistical machine translation: Parameter estimation. *Computational Linguistics*, 19 (2), 263–311.
22. Palmer, M., Gildea, D., Kingsbury, P. (2005). The Proposition Bank: An Annotated Corpus of Semantic Roles. *Computational Linguistics*, 31 (1), 71–106. doi: <https://doi.org/10.1162/0891201053630264>
23. Satyapanich, T., Ferraro, F., Finin, T. (2020). CASIE: Extracting Cybersecurity Event Information from Text. *Proceedings of the AAAI Conference on Artificial Intelligence*, 34 (5), 8749–8757. doi: <https://doi.org/10.1609/aaai.v34i05.6401>
24. Peters, M., Neumann, M., Zettlemoyer, L., Yih, W. (2018). Dissecting Contextual Word Embeddings: Architecture and Representation. *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*. doi: <https://doi.org/10.18653/v1/d18-1179>
25. Roth, M., Lapata, M. (2016). Neural Semantic Role Labeling with Dependency Path Embeddings. *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. doi: <https://doi.org/10.18653/v1/p16-1113>
26. Marcheggiani, D., Titov, I. (2017). Encoding Sentences with Graph Convolutional Networks for Semantic Role Labeling. *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*. doi: <https://doi.org/10.18653/v1/d17-1159>
27. Howard, J., Ruder, S. (2018). Universal Language Model Fine-tuning for Text Classification. *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. doi: <https://doi.org/10.18653/v1/p18-1031>
28. Iter, D., Grangier, D. (2021). On the Complementarity of Data Selection and Fine Tuning for Domain Adaptation. *Computation and Language*. doi: <https://doi.org/10.48550/arXiv.2109.07591>
29. Devlin, J., Chang, M. W., Lee, K., Toutanova, K. (2018). Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint*. doi: <https://doi.org/10.48550/arXiv.1810.04805>
30. Collobert, R., Weston, J., Bottou, L., Karlen, M., Kavukcuoglu, K., Kuksa, P. (2011). Natural language processing (Almost) from scratch. *Journal of machine learning research*, 12, 2493–2537.
31. Schütze, H. (1998). Automatic word sense discrimination. *Computational linguistics*, 24 (1), 97–123.
32. Pennington, J., Socher, R., Manning, C. D. (2014). Glove: Global vectors for word representation. *Proceedings of the 2014 conference on empirical methods in natural language processing*, 1532–1543. doi: <https://doi.org/10.3115/v1/d14-1162>
33. Surdeanu, M., Johansson, R., Meyers, A., Márquez, L., Nivre, J. (2008). The CoNLL 2008 shared task on joint parsing of syntactic and semantic dependencies. *CoNLL 2008: Proceedings of the Twelfth Conference on Computational Natural Language Learning*, 159–177. doi: <https://doi.org/10.3115/1596324.1596352>

34. Shalev-Shwartz, S., Ben-David, S. (2014). *Understanding machine learning: From theory to algorithms*. Cambridge university press. doi: <https://doi.org/10.1017/cbo9781107298019>
35. Zhang, W., Yin, Z., Sheng, Z., Li, Y., Ouyang, W., Li, X. et al. (2022). Graph Attention Multi-Layer Perceptron. *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. doi: <https://doi.org/10.1145/3534678.3539121>
36. Sandhu, A., Edara, A., Narayan, V., Wajid, F., Agrawala, A. (2022). Temporal Analysis on Topics Using Word2Vec. doi: <https://doi.org/10.48550/arXiv.2209.11717>
37. Heimerl, F., Gleicher, M. (2018). Interactive Analysis of Word Vector Embeddings. *Computer Graphics Forum*, 37 (3), 253–265. doi: <https://doi.org/10.1111/cgf.13417>
38. Bojanowski, P., Grave, E., Joulin, A., Mikolov, T. (2017). Enriching Word Vectors with Subword Information. *Transactions of the Association for Computational Linguistics*, 5, 135–146. doi: https://doi.org/10.1162/tacl_a_00051
39. Inoue, N., Shinoda, K. (2016). Adaptation of Word Vectors using Tree Structure for Visual Semantics. *Proceedings of the 24th ACM International Conference on Multimedia*. doi: <https://doi.org/10.1145/2964284.2967226>

Anastasiia Poltorak, Svitlana Tyshchenko, Olha Khrystenko,
Volodimir Ribachuk, Vitalii Kuzoma, Viktoriia Stamat
© The Author(s) 2023

CHAPTER 5

THEORETICAL AND PRAXEOLOGICAL APPROACHES TO MONITORING THE STATE OF FINANCIAL SECURITY OF UKRAINE

ABSTRACT

In today's conditions of globalization and constant changes in the financial market, the issue of preserving financial security is becoming extremely important for every country. Financial security not only determines the stability of the national economy, but is also the basis of the well-being of citizens and the ability of the state to perform its social and economic functions. The purpose of this study is a comprehensive substantiation of the theoretical and methodological foundations and practical methods of monitoring the state of financial security of Ukraine in conditions of economic turbulence as a factor ensuring the preservation of the state's financial system.

Taking into account the fact that the methodical approach to calculating the level of economic security of Ukraine does not involve a regional assessment, a methodical approach to monitoring the security state of the financial stability of the regions has been developed. The given methodological approach includes the following sequence of actions: division of the component "financial security of the region" into subcomponents; creation of a list of indicators for each financial security subsystem of the region; normalization of these indicators within the subsystem, determination of their importance for each separate subsystem of financial security of the region; generalization of indicators into complex indicators for assessing the state of financial security of the region in the context of various subsystems; ranking of regions according to the obtained values; calculation of the integral indicator of the state of financial security for individual regions and research periods, as well as grouping of regions based on the obtained results; comparing the state of financial security of regions based on the calculated values of the integral indicator of the state of financial security and highlighting specific aspects that are specific to each region.

A list of 22 indicators of the state of financial security of regions has been created, which meets the following criteria: it is scientifically based, characterized by the availability of statistical data and suitability for mathematical and other types of analysis, highlighting the change of a phenomenon or process over time, unambiguous interpretation. It is proved that the selected indicators of the state of financial security of the regions are not in a strong relationship, and are also interconnected with the state of financial security of the state, which generally confirms the proposed hypothesis that the formed matrix of data of the identified indicators can characterize the state of financial security of the

region, testify to specific problems and special opportunities in the region, and, accordingly, to be used as input information in the process of calculating the integral indicator of the financial security of the region.

On the basis of the proposed methodology for assessing the state of financial security of regions, integral indicators of the state of financial security of regions of Ukraine were calculated, which are actually the result of collapsing indicators by subsystems into a system index for a certain region, high values of which characterize a relatively stable value of financial security of a certain region, and low values signal its dangerous or critical condition. The regions of Ukraine were clustered according to the ranges of the financial security of the regions, according to the results of which the regions were divided into 4 groups: with a critical state of financial security of the region (0.000–0.381) (Luhansk, Donetsk regions), a dangerous state (0.382–0.499), a satisfactory state (0.500–0.618) and conditionally high (0.619–1.000) (Dnipro, Kyiv, Poltava regions).

KEYWORDS

Economic security, financial security, management of the financial security system, monitoring of financial security, national security.

In today's conditions of globalization and constant changes in the financial market, the issue of preserving financial security is becoming extremely important for every country. Financial security not only determines the stability of the national economy, but is also the basis of the well-being of citizens and the ability of the state to perform its social and economic functions. Since the beginning of the Russian military invasion on February 24, 2022, the National Bank of Ukraine fixed the official exchange rate, and in the summer of 2022 increased it by 25 %, introducing additional restrictions on the foreign exchange market to ensure the macro-financial stability of the state. At the beginning of 2023, the difference between the official and cash exchange rates in Ukraine did not exceed 10–11 %, and market fluctuations were minimal even during massive shelling. Thanks to administrative measures and the support of the international community, it was possible to preserve Ukraine's international reserves. According to data at the end of January 2023, their level (29.9 billion USD) exceeded the volume of reserves before the military invasion by 9 %. So, the financial security of Ukraine is preserved now in extremely difficult conditions. Artificial restrictions that have been introduced in the field of currency security, which is an important component of financial security, work temporarily and may generate new risks over time. To avoid this, the National Bank of Ukraine constantly monitors the situation, analyzes possible scenarios and prepares appropriate solutions.

The purpose of this study is a comprehensive substantiation of the theoretical and methodological foundations and practical methods of monitoring the state of financial security of Ukraine in conditions of economic turbulence as a factor ensuring the preservation of the state's financial system. In accordance with the purpose of the study, the following theoretical, methodological and practical tasks were set: to reveal the conceptual basis for assessing the state of financial security

of the state; to investigate the security condition of the financial system of Ukraine as a basis for ensuring the economic security of the state; to develop a methodological concept for the transformation of approaches to monitoring the financial security of Ukraine.

Scientists, including: S. Akinleye, R. Dauda, O. Iwegbu, O. Popogbe [1], G. Datsenko et al., made a significant contribution to the development of the scientific paradigm of monitoring the security state of the financial system of states [2], N. Davydenko, Yu. Bilyak, Yu. Nehoda, N. Shevchenko [3], K. Garškaitė-Milvydienė, N. Maknickienė, M. Tvaronavičienė [4], Md. Hossain, U. Jahan, R. Rifat, A. Rasel, M. Rahman [5], V. Kovalenko et al. [6], M. Kryshchanovych, R. Shulyar, M. Svitlyk, O. Zorya, N. Fatiukha [7], M. Kynytska-Iliash [8], S. Onyshchenko, I. Shchurov, A. Cherviak, O. Kivshyk [9], P. Panda [10], A. Poltorak, O. Khrystenko, A. Sukhorukova, T. Moroz, O. Sharin [11], N. Reshetnikova, Zh. Gomostaeva, Yu. Chernysheva, I. Kushnareva, E. Alekhina [12], H. Salkić, A. Omerović, A. Salkić, M. Kvasina [13], N. Sirenko et al. [14], N. Vyhovska, I. Voronenko, A. Konovalenko, V. Dovgaliuk, I. Lytvynchuk [15], X. Xie, M. Osińska, M. Szczepaniak [16], S. Yekimov, O. Prodius, T. Chelombitko, A. Dudnyk, V. Chernyak [17], S. Yekimov, V. Purtov, I. Buriak, D. Kabachenko [18], S. Yekimov, V. Sarychev, N. Malyuga, L. Shkulipa [19] and others, the scientific results of which highlight the current conclusions of security theory, the classification of factors and conditions that are a prerequisite for the creation of threats financial security, the role and place of financial security in general theories of international relations.

5.1 CONCEPTUAL BASES FOR ASSESSING THE STATE OF FINANCIAL SECURITY OF THE STATE

The financial security of the country means the state in which the operations of the internal and external financial system do not disrupt the normal functionality of this complex system and do not cause obstacles to the formation of favorable financial conditions for its balanced development. This state can be measured using the aggregation of indicators reflecting the state of monetary, currency, banking, budgetary, tax, debt security, as well as the security of the non-banking financial sector.

Having analyzed the genesis of regulatory and legal provision of financial security, it was found that for the further development of the scientific approach, it is necessary to apply a systematic approach for a deep understanding of the nature of such a complex phenomenon as security, and consider it in various aspects, such as financial, economic, national. This approach will contribute to the creation of a complex systemic regulatory framework that will help implement an effective mechanism for ensuring the country's financial security.

It should be noted that imperative globalization processes are characterized by both unifying and polarizing consequences. Proponents of globalization focus attention on its positive results, noting that globalization is a source of additional freedom and progress, the formation of an impetus for economic development, a global network of information, logistical and transport advantages, the development of the investment mechanism and the acceleration of the introduction of innovations, while opponents of globalization argue that it can cause TNCs to absorb established markets, economic inequality, social tensions, and loss of cultural identity.

The division of the concept of "financial security" was carried out according to the object of protection, and this analysis made it possible to identify the following structural components: financial security of households, business entities, territorial communities, economic sectors, regions, the state and the global financial space. This distribution confirms that financial security actually determines the conditions for the functioning and development of industries and regions, as well as for society as a whole and each of its individuals in particular. At the same time, the financial security of the state combines all accumulated risks, confirming the existence of interdependence between all objects of protection and the general financial security of the country.

The author's view on the systematic taxonomy of the state's financial security and its place in the national security system is presented, in which the state's financial security is conventionally divided into three subsystems: the security of state finances; security of the financial market; cyber security of the financial sector (Fig. 5.1).

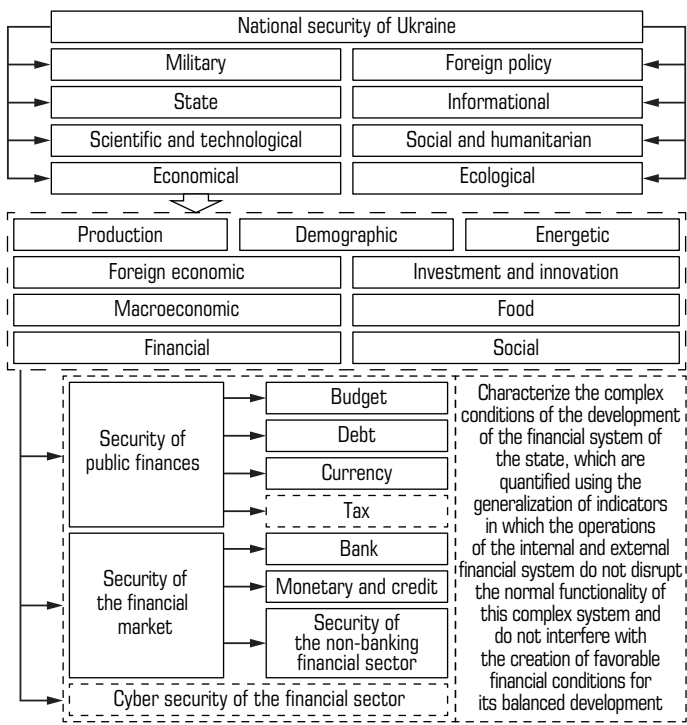


Fig. 5.1 Classification of financial security and its role in the overall structure of the country's national security
 Note: systematized and expanded by the authors

In our opinion, the financial sector is the most vulnerable to cyber attacks. It is financial institutions, given their key role as intermediaries in monetary transactions, that become the main targets for cyber attacks, among which: illegal actions on ATMs, financial transactions, destruction of files, introduction of malicious programs into banking systems, incidents affecting internal processes and extortion. Such attacks can cause significant material losses and harm the reputation of financial institutions. That is why a separate subsystem – "cybernetic security of the financial sector" has been singled out in the structure of financial security.

Let's summarize the indicators of the state of financial security of the state, which are proposed for use by domestic legislation [20], in the **Table 5.1**.

● **Table 5.1** Complex of indicators of the state of financial security of Ukraine

Indicator	Calculation method	Notes
1	2	3
Bank security		
Share of overdue credit debt to the total volume of loans granted by banks to residents of Ukraine, %	$\frac{LA_o}{LA} \times 100 \%$	LA_o – overdue loan debt, million UAH; LA – loans granted to residents of Ukraine, million UAH
Ratio of loans and deposits of banks issued in foreign currency, %	$\frac{LAC}{RDC} \times 100 \%$	LAC – loans granted to residents of Ukraine in foreign currency, million UAH; RDC – deposits raised from residents in foreign currency, million UAH
The specific weight of foreign capital in the total structure of the authorized capital of banking institutions, %	$\frac{FC}{BC} \times 100 \%$	FC – foreign capital in the authorized capital of banks, million UAH; BC – authorized capital of banking institutions, million UAH
Ratio of loans and deposits (long-term), times	$\frac{LA_{1-5} + LA_{>5}}{RD_{1-5} + RD_{>5}}$	LA_{1-5} – loans granted to residents for a term of 1 to 5 years, million UAH; $LA_{>5}$ – loans granted to residents for a term of more than 5 years, million UAH; RD_{1-5} – deposits attracted for a period of 1 to 5 years from residents, million UAH; $RD_{>5}$ – deposits attracted for a period of more than 5 years from residents, million UAH
Return on assets, %	$\frac{BP}{AV_a} \times 100 \%$	BP – bank profit after tax, million UAH; AV_a – value of assets of banking institutions, million UAH
Ratio of liquid assets and liabilities (short-term), %	$\frac{AL}{L_{st}} \times 100 \%$	AL – liquid assets, million UAH; L_{st} – liabilities (short-term), million UAH
The specific weight of the assets of the 5 largest banking institutions in the total assets of the banking system, %	$\frac{BA_5}{BA} \times 100 \%$	BA_5 – volume of assets of the 5 largest banking institutions, million UAH; BA – assets of banks, million UAH

• Continuation of Table 5.1

1	2	3
Security of the financial market (non-banking)		
Insurance penetration level, %	$\frac{GIP}{GDP} \times 100 \%$	<i>GIP</i> – gross insurance premiums, million UAH; <i>GDP</i> – gross domestic product, million UAH
Capitalization level of listed companies, % of GDP	$\frac{CSE}{GDP} \times 100 \%$	<i>CSE</i> – assessment of the market value of capital that is traded on stock exchanges in the form of shares, million UAH
Volatility level of the indicator of the First Stock Trading System (hereinafter - FSTS), the number of critical deviations (–10 %)	$\sum_{t=1}^T K_i; K_i = \begin{cases} 0, & T_p FSTS \geq 90 \% \\ 1, & T_p FSTS < 90 \% \end{cases}$ $T_p FSTS = \frac{FSTS_t}{FSTS_{t-1}} \times 100 \%$	<i>T</i> – every Friday of the period
The specific weight of insurance premium income of the 3 largest insurance companies in the structure of insurance premium income, %	$\frac{IP_3}{IP} \times 100 \%$	<i>IP</i> ₃ – insurance premiums of the 3 largest insurance companies (excluding life insurance), million UAH; <i>IP</i> – insurance premiums, million UAH
Debt security		
Ratio of public debt (state and state-guaranteed) to GDP, %	$\frac{SD}{GDP} \times 100 \%$	<i>SD</i> – amount of public debt, million UAH
Ratio of gross external debt to GDP, %	$\frac{GED \times AR_{UAH}}{GDP} \times 100 \%$	<i>GED</i> – gross external debt, million USD; <i>AR</i> _{UAH} – average exchange rate of the UAH
Weighted average yield of domestic state loan bonds, %	$\frac{\sum_{n=1}^N IB}{n}$	<i>IB</i> – yield on domestic state loan bonds; <i>n</i> – the number of periods
EMBI+Ukraine index (Emerging Markets Bond Index)	weighted average spread of Eurobonds of Ukraine to the yield level of US bonds	
Ratio of international reserves to gross external debt, %	$\frac{RA}{GED} \times 100 \%$	<i>RA</i> – volume of reserve assets, million USD
Budget security		
Ratio of the state budget deficit to GDP, %	$\frac{SB_d}{GDP} \times 100 \%$	<i>SB</i> _d – state budget deficit, million UAH
Deficit of budgetary and extra-budgetary funds of the general government sector, % of GDP	$\frac{SA_d - CB_d}{GDP} \times 100 \%$	<i>SA</i> _d – deficit of the general government sector, million UAH; <i>CB</i> _d – deficit of the consolidated budget, million UAH
GDP redistribution through the combined budget, %	$\frac{CB_r}{GDP} \times 100 \%$	<i>CB</i> _r – revenues of the consolidated budget, million UAH

● Continuation of Table 5.1

1	2	3
Ratio of debt repayment and service payments to state revenues, %	$\frac{SB_s + SB_r}{SBR} \times 100 \%$	SB_s – public debt service, million UAH; SB_r – repayment of public debt, million UAH; SBR – state budget revenues, million UAH
Currency security		
The average change in the exchange rate of the UAH to the USD for the period	$\frac{AR_{UAN n}}{AR_{UAN n-1}}$	$AR_{UAN n}$ – average UAH to USD exchange rate (current year); $AR_{UAN n-1}$ – average UAH to USD exchange rate (previous year)
Gross international reserves of Ukraine, months of imports	$\frac{IR}{AIL}$	IR – international reserves of Ukraine, million USD; AIL – average monthly level of imports, million USD
Share of loans formed in foreign currency in the total amount of loans, %	$\frac{LA_{fc}}{LA} \times 100 \%$	LA_{fc} – loans granted in foreign currency to residents, million UAH
Balance of purchase and sale of foreign currency (by population), billion USD	$C_{sp} - C_{bp}$	C_{sp} – volume of sold currency, billion USD; C_{bp} – volume of purchased currency, billion USD
Dollarization of the money supply, %	$D_{ms} = \frac{TD_{fc} + OD_{fc} + SE_{fc}}{M_3} \cdot 100$	D_{ms} – dollarization of the money supply, %; TD_{fc} – transferable deposits (foreign currency); OD_{fc} – other deposits (foreign currency); SE_{fc} – securities (foreign currency); M_3 – money supply [14]
Monetary and credit security		
The specific weight of cash in the structure of the money supply, %	$\frac{M_0}{M_3}$	M_0 – cash in circulation, million UAH; M_3 – money supply, million UAH
The difference between loan and deposit rates, % of points	$LA_{\%} - RD_{\%}$	$LA_{\%}$ – loan rates, %; $RD_{\%}$ – deposit rates, %
Weighted average interest rate on loans in UAH relative to the consumer price index, % points	$LA_{\%aver} - CPI$	$LA_{\%aver}$ – weighted average interest rate on loans in UAH, %; CPI – consumer price index
Share of consumer loans in their overall structure, %	$\frac{LA_{th}}{LA} \times 100 \%$	LA_{th} – consumer loans granted to households
Share of loans (long-term) in their total amount, %	$\frac{\frac{LA_{>5fc}}{AR_{UAN n}} + LA_{UAH}}{AR_{UAN n-1} / AR_{UAN n-1}} \times 100 \%$	$LA_{>5fc}$ – loans for a term of more than 5 years (foreign currency); LA_{UAN} – loans in national currency for a term of more than 5 years

Note: summarized by the authors

The main methodology, which in the legislative and regulatory space illuminates the mechanisms for assessing the financial security of Ukraine, is presented in the Methodological recommendations [20], approved on October 29, 2013, which have "informational, advisory, explanatory nature and are not mandatory" [20].

The above recommendations summarize the approaches that allow to quantitatively assess the state of economic stability of Ukraine and the level of financial security as its key component. This methodology contains a list of indicators, their recommended values, as well as procedures for calculating the overall indicator of economic security and its components. These methodological recommendations are based on a complex analysis of indicators of economic stability in order to identify possible threats and are used by the Ministry of Economic Development, Trade and Agriculture of Ukraine for a comprehensive assessment of the level of economic security [20]. Accordingly, this technique should be used to monitor the components of financial security in order to make management decisions regarding the analysis, prevention and elimination of real and potential threats in the field of finance.

To assess the level of financial security, it is necessary to assess the state of its components (their integral indices) using the analysis of the values of a set of indicators selected according to the principles of reliability, representativeness and information availability. So, for example, Ukraine's debt security is characterized by a set of numerical indicators that can be highlighted in the form of a vector. The set of indicators (components of the vector) is partly based on statistical data, and partly on data obtained by the method of expert evaluation.

Indicators of the level of financial security of the state are interconnected indicators of the state of the financial system, which quantitatively reflect the level of risk and have a high sensitivity and signaling ability to warn scientists, the state and market participants about probable threats that arise as a result of changes in macroeconomic conditions, and adoption management decisions in the field of finance.

Let's note that for each of the indicators of the state of financial security, the set of which is divided into three types depending on their economic content (stimulators, destimulators, mixed), ranges of characteristic values are defined.

5.2 ANALYSIS OF THE STATE OF FINANCIAL SECURITY OF UKRAINE AS A BASIS FOR ENSURING THE ECONOMIC SECURITY OF THE STATE

The security of state finances is classified into budgetary, debt, currency and tax security of the state, which we have singled out. Taking the above as a basis, let's analyze the state of these subsystems during 2009–2022, using the Methodology [20].

It is advisable to consider the state's debt security as the optimal ratio between borrowing (internal and external) taking into account certain indicators, such as the cost of servicing and the total amount of public debt [21, 22].

Let's analyze the value of the above-mentioned indicators in 2009–2022 and summarize the normalized indicators in the integrated index of the state of debt security for their further forecasting in the medium term. The input data for determining the set of debt security indicators proposed by the Ministry of Economic Development and Trade of Ukraine are presented in the **Table 5.2**.

● **Table 5.2** Input information for calculating indicators of Ukraine's debt security

Years						
GDP of Ukraine, billion UAH						
2009	2010	2011	2012	2013	2014	2015
913.3	1082.6	1316.6	1408.9	1454.9	1566.7	1979.5
2016	2017	2018	2019	2020	2021	2022
2383.2	2982.9	3558.7	3974.6	4194.1	5459.6	5191.0
GDP of Ukraine, billion USD						
2009	2010	2011	2012	2013	2014	2015
117.2	136.4	163.2	175.8	183.3	131.8	90.6
2016	2017	2018	2019	2020	2021	2022
93.3	112.2	130.8	153.8	155.6	199.8	160.5
State debt of Ukraine (state and state-guaranteed), billion UAH						
2009	2010	2011	2012	2013	2014	2015
316.9	432.2	473.1	515.5	584.1	1100.6	1572.2
2016	2017	2018	2019	2020	2021	2022
1929.8	2141.7	2168.6	1998.3	2551.9	2671.8	4071.7
Public debt of Ukraine (state and state-guaranteed), billion USD						
2009	2010	2011	2012	2013	2014	2015
39.69	54.29	59.22	64.50	73.08	69.79	65.51
2016	2017	2018	2019	2020	2021	2022
70.97	76.31	78.32	84.36	90.26	97.95	111.34
Gross foreign debt of Ukraine, billion USD						
2009	2010	2011	2012	2013	2014	2015
103.4	117.3	126.2	135.1	142.1	126.3	118.7
2016	2017	2018	2019	2020	2021	2022
113.5	116.6	114.7	121.7	125.7	129.7	132.0
Official international reserves, billion USD						
2009	2010	2011	2012	2013	2014	2015
26.5	34.6	31.8	24.5	20.4	7.5	13.3
2016	2017	2018	2019	2020	2021	2022
15.5	18.8	20.8	25.3	29.1	30.9	28.5

Note: summarized by the authors based on data [23–25]

Let's present the data on the aggregate state debt of Ukraine in **Fig. 5.2**.

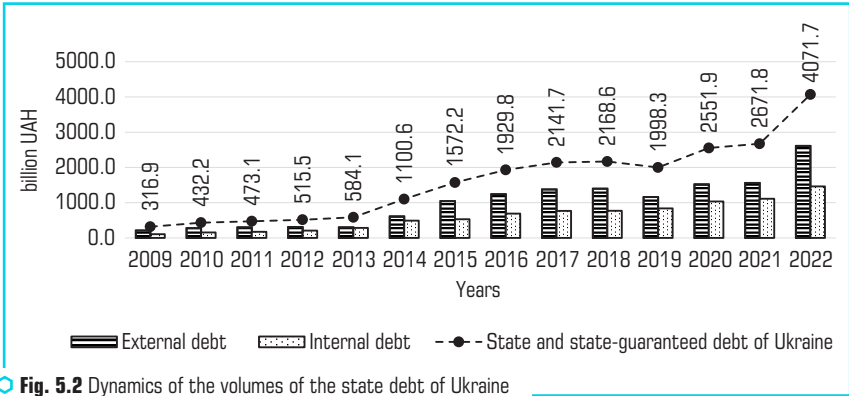


Fig. 5.2 Dynamics of the volumes of the state debt of Ukraine
 Note: calculated by the authors based on [25]

In our opinion, it is appropriate to analyze the dynamics of the gross domestic product of Ukraine simultaneously in the national monetary unit and in USD. Let's highlight the graphically obtained indicators of Ukraine's GDP for 2009–2022 in **Fig. 5.3**.

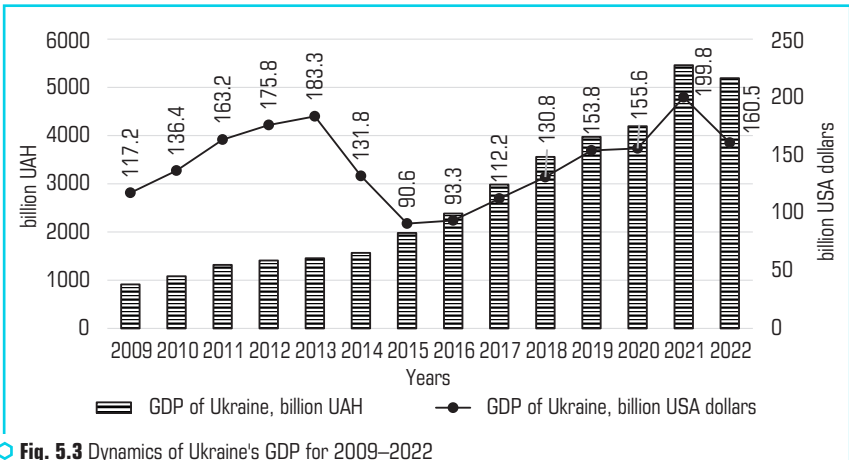


Fig. 5.3 Dynamics of Ukraine's GDP for 2009–2022
 Note: summarized by the authors based on [25]

Analyzing the data of **Fig. 5.3**, it is appropriate to pay attention to the fact that the GDP of the state, calculated in the national monetary unit, has a steady upward trend (from 913.3 billion UAH according to the results of 2009 to 5191.0 billion UAH in 2022). The GDP of Ukraine, defined

in USD, steadily increased during 2009–2013 (from 117.2 billion USD in 2009 to 183.3 billion USD in 2013), in 2014 the indicator decreased to 131, 8 billion USD or by 28 % compared to 2013. During 2015–2017, the studied indicator did not exceed the value of the crisis year of 2009 at all, being in the range of 90.6–106.3 billion USD. As of the end of 2022, the GDP of Ukraine, defined in USD, amounted to 165.5 billion USD. Using the statistical data highlighted in the **Table 5.3**, let's calculate the absolute values of indicators of the state of debt security of Ukraine and present them in the **Table 5.3**.

● **Table 5.3** Dynamics of Ukraine's debt security

Years						
Ratio of public debt (state and state-guaranteed) to GDP, % (α_1)						
2009	2010	2011	2012	2013	2014	2015
34.7	39.9	35.9	36.6	40.1	70.2	79.4
2016	2017	2018	2019	2020	2021	2022
81.0	71.8	60.9	50.3	60.9	48.9	78.4
Ratio of gross external debt to GDP, % (α_2)						
2009	2010	2011	2012	2013	2014	2015
88.2	86.0	77.4	76.8	77.5	95.8	131.0
2016	2017	2018	2019	2020	2021	2022
121.7	103.9	87.7	79.2	80.8	64.8	82.2
Weighted average yield of domestic loan bonds, % (α_3)						
2009	2010	2011	2012	2013	2014	2015
12.2	10.4	9.2	12.9	13.1	13.4	13.1
2016	2017	2018	2019	2020	2021	2022
9.2	10.5	17.8	16.9	10.2	11.3	18.3
EMBI+Ukraine index, % (α_4)						
2009	2010	2011	2012	2013	2014	2015
1606.2	556.0	549.4	765.2	680.9	2226.0	2374.6
2016	2017	2018	2019	2020	2021	2022
590.9	691.4	825.5	770.3	1011.9	1082.0	1093.0
The ratio of international reserves to gross external debt, % (α_5)						
2009	2010	2011	2012	2013	2014	2015
25.63	29.47	25.19	18.17	14.37	5.96	11.20
2016	2017	2018	2019	2020	2021	2022
13.69	16.12	18.15	20.78	23.18	23.85	21.59

Note: calculated by the authors according to the data in the **Table 5.2** based on the methodology [20]

Analytical data of **Table 5.3** show that the ratio of public debt to GDP increased from 34.7 % in 2009 to 78.4 % as of 2022, which exceeds the legally established threshold (critical) level. Let's draw attention to the fact that the value of this indicator has been in a permanently critical state since 2014 (**Fig. 5.4**).



Fig. 5.4 Dynamics of debt dependence of Ukraine
Note: summarized by the authors based on [25]

During the period of sovereign development, in our opinion, there was an atmosphere of too rapid increase in the state's debt obligations, which caused a weakening of the activity of the inflow of foreign investments due to an objective increase in the level of risk for foreign investors. Let's agree with the opinion about the emergence of a debt spiral, i.e. a situation where the budget deficit requires additional government borrowing, accordingly, the public debt and the costs of its maintenance increase, which again cause the budget deficit [26].

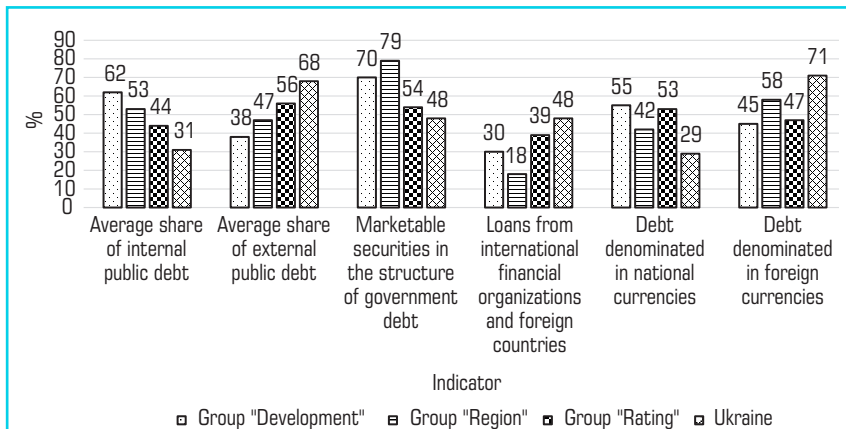
Having analyzed the comparative data on the size of the public debt of different countries of the world and their credit ratings, as well as the data of the medium-term Strategy for the management of the public debt of Ukraine for 2021–2024 [21], 15 peer countries (**Table 5.4**) were selected for the analysis of the level of debt dependence (**Fig. 5.5**).

Comparing the structure of the total debt of Ukraine and the average similar indicators for the formed groups of countries (**Fig. 5.5**), there are indisputable statements that the indicator of the specific weight of external public debt in Ukraine (78.4 %) is significantly higher than the average indicators in the three analysis groups (38–56 %), in addition, the structure of public debt by instruments also has its own characteristics: the specific weight of marketable securities is lower than the average indicators of analytical groups, and the non-marketable public debt, on the contrary, is higher.

● **Table 5.4** The set of countries selected for comparison of levels of debt dependence of Ukraine, 2023

Developing countries that significantly influence the economic development of their region ("Development" group)			Countries selected by the criterion of geographical proximity to Ukraine ("Region" group)			Countries with similar credit ratings of international rating agencies ("Rating" group)		
S&P	Moody's	Fitch	S&P	Moody's	Fitch	S&P	Moody's	Fitch
Turkey			Poland			Pakistan		
BB-	Ba2	BB+	BBB+	A2	A-	B	B3	B
Nigeria			Bulgaria			Macedonia		
B	B2	B+	BBB-	Baa2	BBB	BB-	NR	BB+
Thailand			Croatia			Iraq		
BBB+	Baa1	BBB+	BB+	Ba2	BB+	B-	Caa1	B-
Uruguay			Czech Republic			Lebanon		
BBB	Baa2	BBB-	AA-	A1	A+	B-	B3	B-
			Serbia			Ghana		
			BB	Ba3	BB	B-	B3	B
			Hungary			Ukraine		
			BBB-	Baa3	BBB-	B-	Caa2	B-

Note: created by the author using data [21] and rating agencies S&P, Moody's, Fitch



● **Fig. 5.5** Comparative data on the structure of the total debt of Ukraine and similar countries by group, 2023

Note: created by the author using data [21] and rating agencies S&P, Moody's, Fitch

Loans from international financial organizations and governments of foreign countries in the structure of the total public debt of Ukraine make up 48 %, which is significantly more compared to the average indicators of all comparison groups. The structure of state debt in relation to currency

is also highlighted. Thus, Ukraine recorded the lowest rate of public debt denominated in the national currency (29 %), compared to the average rates for all analytical groups (42–55 %), which definitely increases currency risks. In international practice, the analysis of the level of foreign debt per person is also used. Note that Ukraine's gross external debt per person increased from 2,245.3 USD in 2009 to 3207.8 USD in 2023. Let's present the dynamics of normalized values of indicators of Ukraine's debt security for 2009–2023 in the **Table 5.5**.

● **Table 5.5** Dynamics of normalized values of indicators of Ukraine's debt security

Years						
Ratio of public debt (state and state-guaranteed) to GDP, % (x_1)						
2009	2010	2011	2012	2013	2014	2015
0.71	0.60	0.68	0.67	0.60	0.17	0.15
2016	2017	2018	2019	2020	2021	2022
0.15	0.17	0.20	0.39	0.20	0.42	0.15
Ratio of gross external debt to GDP, % (x_2)						
2009	2010	2011	2012	2013	2014	2015
0.16	0.16	0.18	0.18	0.18	0.15	0.11
2016	2017	2018	2019	2020	2021	2022
0.12	0.13	0.16	0.18	0.17	0.30	0.17
Weighted average yield of domestic loan bonds, % (x_3)						
2009	2010	2011	2012	2013	2014	2015
0.18	0.26	0.38	0.17	0.16	0.16	0.17
2016	2017	2018	2019	2020	2021	2022
0.16	0.25	0.12	0.13	0.28	0.19	0.12
EMBI+Ukraine index, % (x_4)						
2009	2010	2011	2012	2013	2014	2015
0.12	0.54	0.55	0.36	0.42	0.09	0.08
2016	2017	2018	2019	2020	2021	2022
0.51	0.46	0.32	0.35	0.20	0.18	0.18
Ratio of international reserves to gross external debt, % (x_5)						
2009	2010	2011	2012	2013	2014	2015
0.27	0.32	0.27	0.18	0.14	0.06	0.11
2016	2017	2018	2019	2020	2021	2022
0.14	0.16	0.18	0.21	0.24	0.25	0.22
Integrated index of debt security, % (x_6)						
2009	2010	2011	2012	2013	2014	2015
0.30	0.38	0.41	0.32	0.30	0.13	0.12
2016	2017	2018	2019	2020	2021	2022
0.21	0.23	0.19	0.25	0.22	0.28	0.17

Note: calculated by the authors taking into account the methodology [20]

Therefore, having studied the state and trends of debt security of Ukraine, let's come to the conclusion that the vast majority of indicators of the state of debt security during the last period are in the zone of critical values, which confirms the negative influence of the state of debt security of the state on the level of its financial security [27, 28].

Let's analyze the state of budget security of Ukraine for 2009–2022 and summarize the results of the analysis in **Table 5.6**.

The intense hostilities in Ukraine, which began on February 24, 2022, led to the fact that the Government immediately introduced a number of measures in connection with martial law. Among these measures was the reorientation of the country's budget to military needs and spending on the most necessary social and humanitarian goals, which are aimed at supporting the population and internally displaced persons, as well as ensuring the operation of critical infrastructure. Due to a shortage of domestic resources in a war-torn economy, significant amounts of foreign aid from international partners have helped to finance priority expenditures on time and in full, including pensions, social benefits, salaries of medical and educational personnel, as well as spending on security, defense, health care, self and education [29].

● **Table 5.6** Dynamics of the state of budgetary security of Ukraine

Years						
Ratio of deficit/surplus of the state budget to GDP, % (x_1)						
2009	2010	2011	2012	2013	2014	2015
-3.89	-5.94	-1.79	-3.79	-4.45	-4.98	-2.28
2016	2017	2018	2019	2020	2021	2022
-2.94	-1.60	-1.66	-1.96	-5.18	-3.63	-17.62
Deficit of budgetary and extra-budgetary funds of the general government sector, % of GDP (x_2)						
2009	2010	2011	2012	2013	2014	2015
-2.02	-0.71	-0.86	-0.53	0.05	-0.23	-0.11
2016	2017	2018	2019	2020	2021	2022
0.13	0.03	-0.21	-0.01	-0.31	1.06	9.25
GDP redistribution through the combined budget, % (x_3)						
2009	2010	2011	2012	2013	2014	2015
29.89	29.05	30.27	31.62	30.43	29.11	32.94
2016	2017	2018	2019	2020	2021	2022
32.84	34.09	33.28	32.45	32.82	30.45	42.31
The ratio of service payments and repayment of the state debt to budget revenues, % (x_4)						
2009	2010	2011	2012	2013	2014	2015
18.54	17.02	26.86	26.76	33.58	47.42	59.22
2016	2017	2018	2019	2020	2021	2022
37.48	59.80	37.80	46.67	47.21	46.61	34.43

Note: calculated and systematized by the authors based on the methodology [20]

Let's present the normalized indicators of budget security of Ukraine for 2009–2022 and summarize the results of the analysis in **Table 5.7**.

● **Table 5.7** State dynamics of normalized indicators of budget security of Ukraine

Years						
Ratio of the state budget deficit to GDP, % (α_1)						
2009	2010	2011	2012	2013	2014	2015
0.62	0.21	1.00	0.64	0.51	0.40	0.94
2016	2017	2018	2019	2020	2021	2022
0.81	1.00	1.00	1.00	0.36	0.70	0.05
Deficit of budgetary and extra-budgetary funds of the general government sector, % of GDP (α_2)						
2009	2010	2011	2012	2013	2014	2015
1.00	0.86	0.83	0.89	1.00	0.95	0.98
2016	2017	2018	2019	2020	2021	2022
0.96	0.99	0.96	1.00	0.94	0.82	0.11
GDP redistribution through the combined budget, % (α_3)						
2009	2010	2011	2012	2013	2014	2015
0.81	0.90	0.78	0.69	0.77	0.89	0.60
2016	2017	2018	2019	2020	2021	2022
0.61	0.49	0.57	0.64	0.61	0.77	0.17
The ratio of payments for repayment and maintenance of the state debt to budget revenues, % (α_4)						
2009	2010	2011	2012	2013	2014	2015
0.17	0.19	0.12	0.12	0.10	0.07	0.05
2016	2017	2018	2019	2020	2021	2022
0.09	0.05	0.08	0.07	0.07	0.07	0.09
Integral indicator of budget security of Ukraine, % (α_5)						
2009	2010	2011	2012	2013	2014	2015
0.64	0.52	0.68	0.58	0.58	0.56	0.64
2016	2017	2018	2019	2020	2021	2022
0.61	0.64	0.65	0.67	0.48	0.58	0.10

Note: calculated and systematized by the authors based on the methodology [20]

During 2022, the arrival of international financial aid and the recovery of export earnings contributed to the maintenance of relative macro-financial stability and the gradual stabilization of inflationary and devaluation expectations due to the reduction of volatility in the foreign exchange market.

As of January 1, 2023, international reserves of Ukraine amounted to 28.5 billion USD. During 2022, international reserves decreased by 7.9 %, but foreign currency receipts from international partners made it possible to form the volume of international reserves, which corresponded

to 3.6 months of future imports. According to the results of 2022, the surplus of the current account of the balance of payments amounted to 8.6 billion USD. This was largely the result of receiving grants from international partners and the reduction of payments for investment income. The negative balance of trade in goods and services increased due to a sharp decrease in exports of goods and services by 29.9 %, while imports decreased by only 3.9 %.

Therefore, the security level of the budgetary sphere of Ukraine during the analysis period ranged from 64 % in 2009 to 10 % according to the results of 2022, which is characterized as a critical value of the security state of the budgetary sphere of Ukraine.

The next subsystem of the security of state finances and, accordingly, the financial security of Ukraine, the state of which must be analyzed, is currency security, which in the official methodology of the Ministry of Economic Development and Trade is considered as the state of exchange rate formation, which is characterized by the stability of the national currency and the trust of the population in it, and in in which the conditions for attracting foreign investments, progressive development of the economy, and integration aspects are being formed in the state [20].

The first indicator of assessing the state of currency security is the average indicator of changes in the official exchange rate of the UAH to the USD, which is determined by dividing the average official exchange rate in the current period by a similar indicator in the previous period (**Fig. 5.6**).

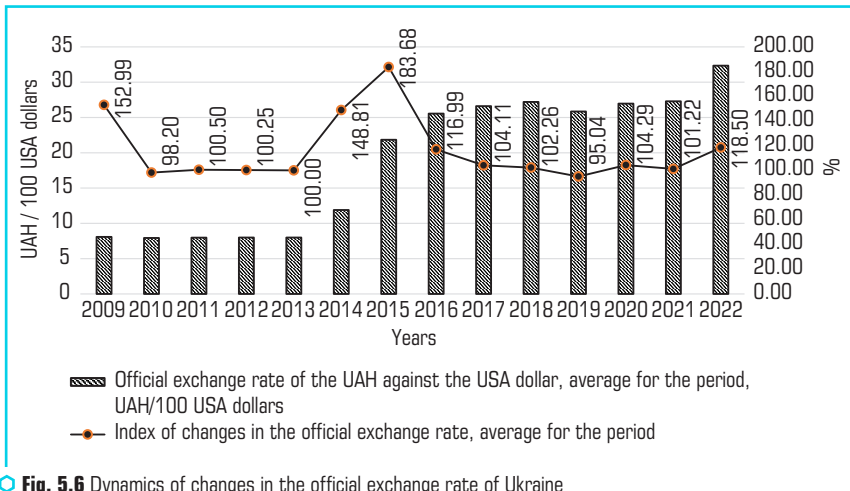


Fig. 5.6 Dynamics of changes in the official exchange rate of Ukraine
Note: summarized by the authors based on data [24]

It should be noted that during the war, the fixed exchange rate made it possible to preserve the stability of the financial system, and for the population and business to partially adapt to life in extremely difficult crises. Over time, these restrictions have caused more problems than good. In 2023, the exchange rate of the national currency is already determined according to general

practice based on the exchange rate for currency transactions on the interbank market. The main prerequisite for such changes was a slowdown in inflation. The second prerequisite was significant foreign exchange reserves of more than 40 billion USD. The third prerequisite was the yield level of UAH deposits (about 15 %), which covers both inflation and exchange rate fluctuations. Let's note that the National Bank cites the accumulation of imbalances in the national economy among the reasons for the above-mentioned changes. An artificially strong national currency significantly reduces the income of exporters and the income of the state budget. In addition, in the conditions of martial law, the vast majority of budget expenditures, which are not directly related to the defense of the state, are financed with the help of international partners, which comes in foreign currency. Accordingly, a weaker UAH makes aid from international partners larger in UAH equivalent, and the government gains room for maneuvers with the financing of social expenditures due to the exchange rate difference.

The next indicator of Ukraine's foreign exchange security status highlights information on Ukraine's gross international reserves, expressed in months of imports (**Fig. 5.7**).



Fig. 5.7 Dynamics of Ukraine's international reserves

Note: summarized by the authors based on data [24]

According to the Methodology [20], the optimal value of this indicator is 5 months, and the range of values [3; 5] is considered satisfactory. Therefore, even during the war period, as of the end of 2022, international reserves amount to 28.5 billion USD, which corresponds to 4.08 months of imports. The next disincentive indicator of the currency security of Ukraine is the share of foreign currency loans in the total volume of loans. According to the results of expert assessment, it is considered that the optimal value of this indicator should not exceed 20 % [20], while a value of 50 % indicates a critical state of this indicator. For the period 2016–2018, the value of the indicator exceeds 40 %, which signals a dangerous or even critical state of the indicator (**Fig. 5.8**).

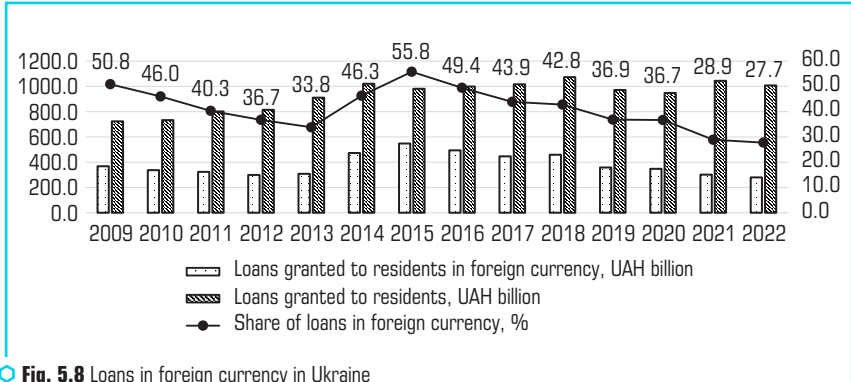


Fig. 5.8 Loans in foreign currency in Ukraine
 Note: calculated by the authors based on data [24]

The next indicator of the mixed type of state of currency security of the state in the system of its financial security is the balance of purchase and sale of foreign currency by the population, the optimal value of which is a value close to zero. This indicator is calculated in billion USD by subtracting the amount of currency bought by the population from the amount of currency sold. The peculiarity of the dynamics of the values of this indicator is that during 2009–2013 the volume of sold currency exceeded the volume of purchased currency in the population and the balance of this value was in the range [2.9; 13.4], and since 2014 the situation has changed, and exceeded the amount of currency purchased from the population. Despite this feature, the normalized values of the indicator during the entire period under study are in the zone of dangerous and critical values, which indicates the presence of certain problems in the process of ensuring the currency security of the state.

The indicator-disincentive of the security state of the currency sphere is the dollarization of the money supply (5.1), the optimal value of which should not exceed 15 %, while a value of 30 % is already considered critical in the process of analyzing the state of financial security of Ukraine:

$$D_{ms} = \frac{TD_{fc} + OD_{fc} + SE_{fc}}{M_3} \cdot 100, \tag{5.1}$$

where D_{ms} – dollarization of the money supply, %; TD_{fc} – transferable deposits (foreign currency); OD_{fc} – other deposits (foreign currency); SE_{fc} – securities (foreign currency); M_3 – money supply [20].

Let's summarize the obtained values of indicators of the state of currency security of Ukraine for 2009–2022 in the **Table 5.8**.

It is impossible to ignore the systematization of the received normalized values of indicators of the state of currency security of Ukraine for 2009–2022 (**Table 5.9**), which will be summarized in the integral index of currency security of the corresponding period.

Therefore, there is an indisputable statement that during the studied period, the state of currency security cannot be assessed as satisfactory. A positive trend, in our opinion, was the upward dynamics of the integral indicator of the state of currency security during 2014–2021, accordingly, it is possible to speak with caution about positive trends and strengthening of the state of currency security, however, military actions on the territory of Ukraine have catastrophically worsened and the state of currency security of Ukraine.

● **Table 5.8** Dynamics of the state of currency security of Ukraine

Years						
Change in the official exchange rate of the UAH to the USD, average for the period (x_1)						
2009	2010	2011	2012	2013	2014	2015
152.99	98.20	100.50	100.25	100.00	148.81	183.68
2016	2017	2018	2019	2020	2021	2022
116.99	104.11	102.26	95.04	104.29	101.22	118.50
Gross international reserves of Ukraine, months of imports (x_2)						
2009	2010	2011	2012	2013	2014	2015
2.80	4.40	3.80	3.00	3.50	1.80	3.00
2016	2017	2018	2019	2020	2021	2022
3.00	3.20	3.30	4.90	4.80	3.80	4.08
Share of foreign currency loans in the total volume of loans, % (x_3)						
2009	2010	2011	2012	2013	2014	2015
50.85	46.03	40.31	36.75	33.82	46.31	55.81
2016	2017	2018	2019	2020	2021	2022
49.43	43.87	42.78	36.85	36.68	28.90	27.73
Balance of purchase and sale of foreign currency (by population), billion USD (x_4)						
2009	2010	2011	2012	2013	2014	2015
0.57	-9.70	-13.40	-10.20	-1.20	2.40	1.50
2016	2017	2018	2019	2020	2021	2022
2.50	2.10	1.50	0.20	1.10	1.20	23.10
Dollarization of the money supply, % (x_5)						
2009	2010	2011	2012	2013	2014	2015
29.1	29.1	30.4	32.1	27.2	32.6	32.2
2016	2017	2018	2019	2020	2021	2022
32.9	31.9	29.2	28.7	26.9	23	32

Note: calculated by the authors based on the methodology [20]

● **Table 5.9** Dynamics of normalized values of indicators of the state of currency security of Ukraine

Years						
The average change in the exchange rate of the UAH to the USD for the period (α_1)						
2009	2010	2011	2012	2013	2014	2015
0.17	1.00	1.00	1.00	1.00	0.17	0.14
2016	2017	2018	2019	2020	2021	2022
0.35	0.99	1.00	0.98	0.97	1.00	0.33
Gross international reserves of Ukraine, months of imports (α_2)						
2009	2010	2011	2012	2013	2014	2015
0.72	0.94	0.88	0.80	0.85	0.32	0.80
2016	2017	2018	2019	2020	2021	2022
0.80	0.82	0.83	0.99	0.98	0.88	0.91
The share of foreign currency loans in the total volume of loans, % (α_3)						
2009	2010	2011	2012	2013	2014	2015
0.20	0.36	0.52	0.61	0.69	0.36	0.18
2016	2017	2018	2019	2020	2021	2022
0.22	0.43	0.46	0.60	0.61	0.82	0.85
Balance of purchase and sale of foreign currency (by population), billion USD (α_4)						
2009	2010	2011	2012	2013	2014	2015
0.98	0.05	0.03	0.04	0.95	0.90	0.94
2016	2017	2018	2019	2020	2021	2022
0.90	0.92	0.94	0.99	0.96	0.95	0.05
Dollarization of the money supply, % (α_5)						
2009	2010	2011	2012	2013	2014	2015
0.26	0.26	0.20	0.19	0.39	0.18	0.19
2016	2017	2018	2019	2020	2021	2022
0.18	0.19	0.25	0.29	0.41	0.65	0.19
Integral index of currency security, % (α_6)						
2009	2010	2011	2012	2013	2014	2015
0.41	0.47	0.47	0.47	0.67	0.34	0.40
2016	2017	2018	2019	2020	2021	2022
0.43	0.59	0.61	0.67	0.68	0.75	0.40

Note: calculated by the authors according to the information in the **Table 5.8** based on the methodology [20]

The main idea of the structure of the financial security of Ukraine proposed by us is that the security of the financial market, as an important component of the financial security of the state, consists of the security of the banking sphere, the monetary sphere and the sphere of the non-banking financial sector. Accordingly, it is time to review the state of these components, the results of which will be the basis for developing strategic vectors for improving the state of security of the financial market of Ukraine and, accordingly, its financial security. Developed and efficient insurance companies, banking institutions and other elements of the financial market are a guarantee of the development of the state's financial system.

The first component of the security of the financial market is banking security of Ukraine, which in the methodology of the Ministry of Economic Development and Trade is considered as the level of financial stability of banking institutions, which, regardless of the conditions of the functioning of the banking system, forms the possibility of its protection from destabilizing factors [20].

One of the priority indicators of the state of banking security, which characterizes certain trends regarding changes in its level, is the specific weight of overdue debt on loans (x_1), the optimal value of which is set at the level of 2 %, and the critical value at the level of 7 %.

The military aggression against Ukraine caused, among other things, the cessation of the long-term trend of a gradual decrease in the share of non-performing loans (NPL), which was observed since 2018. During this period, the volume of NPLs decreased by almost 300 billion UAH, and their share in the loan portfolio decreased from 55 % to 27 % as of March 1, 2022. From March to May 2022, the share of non-performing loans remained almost stable, taking into account the change in regulatory requirements for credit risk assessment. From June 2022, banking institutions began to recognize NPLs. As of January 1, 2023, the share of non-performing loans increased to 38 %, and the total amount of non-performing loans from March to December 2022 increased by 127 billion UAH and amounted to 432 billion UAH.

One of the indicators of the state of banking security of the state according to the Methodology [20] is the ratio of loans and deposits issued by banking institutions in foreign currency. It is quite logical that the optimal range for this indicator is a value close to 100 %, and more precisely the range from 90 % to 110 %. Note that absolutely dangerous values for this mixed type indicator are values lower than 50 % and higher than 180 %. Let's note that according to the results of 2022, this indicator was only 40.86 %, which corresponds to a critical level.

The ratio of foreign capital in the authorized capital of banking institutions is also determined as an indicator, the analysis of which makes it possible to assess the state of banking security of the state. So, the optimal range for this mixed-type indicator is considered to be from 20 % to 25 %. The results of monitoring the state and development of trends in the increase of foreign capital in the total authorized capital of banking institutions prove that in 2015–2017, about half of the available authorized capital of banks was formed at the expense of foreign capital, which was a dangerous signal for forecasting and assessing the state of banking security in Ukraine. During 2018–2021, it was at the level of 28 %, which corresponded to a satisfactory level of

banking security. According to the results of 2022, the share of foreign capital in the authorized capital of banking institutions was 14.3 %.

In order to carry out a comprehensive assessment of the state of banking security in Ukraine, the ratio of long-term loans and deposits is also calculated. The optimal value of the indicator should not exceed one, and a value close to 3 is considered critical. Thus, the normalized values of the indicator provide grounds for concluding that since 2015 the values have been in the range of critical indicators that ensure the level of banking security in this area at a level no higher 20 %. Thus, according to the results of 2022, long-term loans exceeded long-term deposits by 3.6 times, which signals the distrust of the stakeholders of the banking system in keeping funds in it.

A mixed-type indicator in the process of analyzing the state of banking security in Ukraine is the profitability of the assets of banking institutions for the corresponding period, the optimal values of which should be in the range [1; 1.5]. The analysis revealed that the actual values of the indicator approached the optimal range only in 2018, in which the return on assets was 1.7 %, which corresponds to 92 % of the safety level of this indicator. The minimum value of the analyzed indicator was recorded in 2016 and was -12.6 %.

The ratio of liquid assets of banking institutions to their short-term liabilities of the corresponding period is considered in the process of assessing the state of banking security as the sixth indicator of a mixed type, the optimal values of which should be close to unity. This indicator is one of the economic norms established by the NBU for the purpose of control. It defines the minimum actual volume of assets to effectively ensure the fulfillment of obligations. The NBU regulations stipulate that the value of this indicator should not be less than 60 %. It should be noted that in the Methodology of the Ministry of Economic Development and Trade [20] 60 % is a value that is actually in the range of critical values.

One of the indicators for assessing the state of banking security is the specific weight of the assets of the 5 largest banking institutions in the total assets of the state's banking system. As of January 1, 2023, the largest banking institutions were four banks with a state share: JSC KB "PrivatBank" (total assets – 734.413 billion UAH), JSC "Oschadbank" (total assets – 298.158 billion UAH), JSC "Ukreximbank" (total assets – 256.500 billion UAH), JSC "Ukrigasbank" (total assets – 146.351 billion UAH), as well as one bank of foreign banking groups JSC "Raiffeisen Bank Aval" (total assets – 187.290 billion UAH). Accordingly, according to the results of 2022, the total assets of these 5 largest banking institutions amounted to 1,622.712 billion UAH, or 68.94 % of all bank assets.

System data on the state and certain trends of changes in the level of banking security indicators are presented in the **Table 5.10**.

Values of indicators of banking security in accordance with the approved methodology [20] should be translated into normalized values, which are calculated and systematized in the **Table 5.11**.

Fig. 5.9 presents the dynamics of the values of the integral index of banking security of Ukraine for 2009–2022 and the forecast made using the polynomial trend line of the 6th degree ($R^2=0.68$).

● **Table 5.10** Dynamics of the absolute values of indicators of the banking security of Ukraine

Years						
Share of overdue credit debt to the total volume of loans granted by banks to residents of Ukraine, % (x_1)						
2009	2010	2011	2012	2013	2014	2015
5.64	11.20	9.60	8.90	10.90	16.30	24.80
2016	2017	2018	2019	2020	2021	2022
28.20	54.50	52.80	48.40	41.00	30.00	38.00
Ratio of loans and deposits of banks issued in foreign currency, % (x_2)						
2009	2010	2011	2012	2013	2014	2015
215.94	190.20	153.00	118.80	124.10	152.70	168.60
2016	2017	2018	2019	2020	2021	2022
134.50	109.40	117.00	83.50	68.50	62.00	40.86
The specific weight of foreign capital in the general structure of the authorized capital of banking institutions, % (x_3)						
2009	2010	2011	2012	2013	2014	2015
36.70	40.60	41.90	39.50	34.00	32.50	44.00
2016	2017	2018	2019	2020	2021	2022
48.80	48.80	28.00	28.70	28.10	28.00	14.30
Ratio of loans and deposits (long-term), times (x_4)						
2009	2010	2011	2012	2013	2014	2015
6.17	3.75	3.10	2.37	1.76	2.83	3.89
2016	2017	2018	2019	2020	2021	2022
4.13	3.28	3.80	3.80	3.30	3.50	3.60
Return on assets, % (x_5)						
2009	2010	2011	2012	2013	2014	2015
-4.38	-1.50	-0.80	0.50	0.10	-4.07	-5.50
2016	2017	2018	2019	2020	2021	2022
-12.60	-1.90	1.70	4.30	2.40	4.10	-0.50
Ratio of liquid assets and liabilities (short-term), % (x_6)						
2009	2010	2011	2012	2013	2014	2015
35.88	91.19	94.73	90.28	89.11	86.14	92.87
2016	2017	2018	2019	2020	2021	2022
92.09	98.37	93.50	91.00	86.80	89.10	85.90
The specific weight of the assets of the 5 largest banking institutions in the total assets of the banking system, % (x_7)						
2009	2010	2011	2012	2013	2014	2015
32.54	37.00	36.60	38.60	40.00	43.40	53.6
2016	2017	2018	2019	2020	2021	2022
55.6	59.7	60.2	61.4	58.7	55.4	68.94

Note: calculated by the authors

● **Table 5.11** Dynamics of normalized values of indicators of the state of banking security of Ukraine

Years						
1	2	3	4	5	6	7
Share of overdue credit debt to the total volume of loans granted by banks to residents of Ukraine, % (α_1)						
2009	2010	2011	2012	2013	2014	2015
0.34	0.13	0.15	0.16	0.13	0.09	0.06
2016	2017	2018	2019	2020	2021	2022
0.05	0.03	0.03	0.03	0.03	0.05	0.04
Ratio of loans and deposits of banks issued in foreign currency, % (α_2)						
2009	2010	2011	2012	2013	2014	2015
0.17	0.19	0.47	0.91	0.86	0.47	0.31
2016	2017	2018	2019	2020	2021	2022
0.71	1.00	0.93	0.46	0.22	0.28	0.16
The specific weight of foreign capital in the total structure of the authorized capital of banking institutions, % (α_3)						
2009	2010	2011	2012	2013	2014	2015
0.53	0.39	0.39	0.42	0.64	0.70	0.36
2016	2017	2018	2019	2020	2021	2022
0.31	0.31	0.88	0.85	0.88	0.88	0.54
Ratio of loans and deposits (long-term), times (α_4)						
2009	2010	2011	2012	2013	2014	2015
0.10	0.16	0.19	0.36	0.61	0.24	0.15
2016	2017	2018	2019	2020	2021	2022
0.15	0.18	0.16	0.16	0.18	0.17	0.17
Return on assets, % (α_5)						
2009	2010	2011	2012	2013	2014	2015
0.05	0.13	0.24	0.80	0.64	0.05	0.04
2016	2017	2018	2019	2020	2021	2022
0.02	0.11	0.92	0.16	0.64	0.17	0.30
Ratio of liquid assets and liabilities (short-term), % (α_6)						
2009	2010	2011	2012	2013	2014	2015
0.02	0.01	0.01	0.01	0.01	0.01	0.01
2016	2017	2018	2019	2020	2021	2022
0.01	0.01	0.01	0.01	0.01	0.01	0.01
The specific weight of the assets of the 5 largest banking institutions in the total assets of the banking system, % (α_7)						
2009	2010	2011	2012	2013	2014	2015
0.90	0.72	0.74	0.66	0.60	0.53	0.33
2016	2017	2018	2019	2020	2021	2022
0.29	0.21	0.20	0.20	0.23	0.29	0.02

Continuation of Table 5.11

1	2	3	4	5	6	7
Integrated index of banking security, % (α_6)						
2009	2010	2011	2012	2013	2014	2015
0.29	0.24	0.31	0.47	0.50	0.29	0.18
2016	2017	2018	2019	2020	2021	2022
0.22	0.26	0.45	0.26	0.31	0.26	0.18

Note: calculated and systematized by the authors according to the data in the **Table 5.10** based on the methodology [20]

So, having carried out a comprehensive assessment of the state of financial security of Ukraine for 2009–2022, let's summarize the normalized values of the integral index of the security state of the financial system of Ukraine in **Fig. 5.10**.

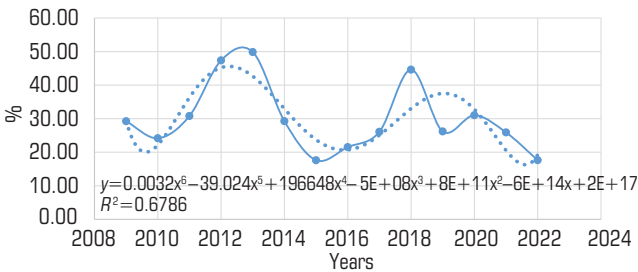


Fig. 5.9 Dynamics of values of the integral index of banking security of Ukraine
 Note: presented by the authors according to the data in the **Table 5.11** based on the methodology [20]

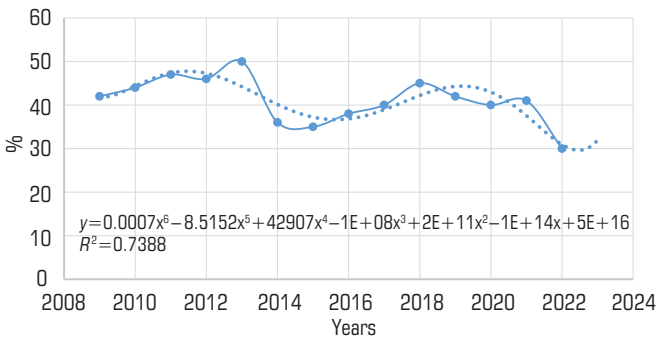


Fig. 5.10 Dynamics of the integral index of the security state of the financial system of Ukraine, %
 Note: calculated by the authors

Therefore, the data obtained in the process of calculations testify to the dangerous state of financial security of Ukraine.

5.3 METHODOLOGICAL CONCEPT OF TRANSFORMATION OF APPROACHES TO MONITORING THE STATE OF FINANCIAL SECURITY OF UKRAINE

The methodology of the Ministry of Economic Development and Trade of Ukraine, which in the legislative and regulatory space of Ukraine is the main methodology that illuminates the mechanisms of assessing the economic security of Ukraine, the structural element of which is financial security, was studied. The shortcomings of this technique, which cause incorrect results of assessing the state of financial security, are outlined, and directions for its improvement are proposed, including:

1. Timely revision of weighting coefficients, which numerically characterize the importance of a certain indicator in comparison with other indicators of the state of financial security.

Among the available methods for calculating the weighting coefficients, the method of sensitivity theory is the most optimal. The use of this method is recommended when there is a macroeconomic model, the initial data of which are indicators of the level of financial security of the state and its subsystems. Thus, the weighting factors for individual indicators (a_i) are determined by assessing how much the integral indicator (D_i) reacts to changes in the normalized state indicators of financial security subsystems (y_i) (5.2):

$$a_i = \frac{|D_i \Delta y_i|}{\sum_{i=1}^n |D_i \Delta y_i|}. \quad (5.2)$$

Using the method of the sensitivity theory to determine the weighting coefficients provides an opportunity to specify these coefficients in different periods of the study, which can be an advantage of this method, in our opinion. However, it is worth considering that using this method can significantly complicate the process of assessing financial security, requiring additional effort and time.

In the case when there is no macroeconomic model that has indicators of financial security and its subsystems as input data, the method of principal components is used to calculate the weighting coefficients (5.3), the input data of which are the dynamic series of certain indicators:

$$a_i = \frac{c_i |d_i|}{\sum c_i |d_i|}, \quad (5.3)$$

where c_i – contribution of indicator i to the total variance of a set of indicators; d_i – factor loadings [30].

Using the method of principal components, it is possible to obtain weighting coefficients with fixed values that remain constant throughout the study period. This, in our opinion, can cause a distortion of the evaluation results. Correlation-regression analysis and statistical approaches, as a rule, reveal general patterns without paying attention to the peculiarities of specific periods, such as crisis moments.

Game methods can also be used in the calculations of weighting factors to assess the financial security of the state. Subsystems of financial security are presented in the form of matrices, where rows correspond to different time periods, and columns reflect normalized indicators for these subsystems. The resulting matrices for financial security subsystems are considered as matrices of a zero-sum game, where the gain of the first player is equal to the loss of the second. After determining the optimal mixed strategies for both players (F_1, F_2), the second mixed strategy can be considered as a certain set of weighting coefficients in the calculation of the general indicator of the state of financial security of the country (FS_j) in the additive form (5.4):

$$FS_j = \sum_{i=1}^n (F_2^i) y_{ij}, \tag{5.4}$$

or in multiplicative form (5.5):

$$FS_j = \prod_{i=1}^n y_{ij}^{(F_2^i)}. \tag{5.5}$$

Therefore, analyzing the existing methods for calculating the weighting coefficients of indicators of the country's financial stability, it is possible to conclude that depending on the specific stages of economic development, different approaches to determining these coefficients can be used. Possible methods include expert judgments, game approaches, principal component methods, and sensitivity theory methods, each with its own advantages and limitations.

2. The maximum replacement of the use of subjective expert evaluations in the process of calculating weighting coefficients of indicators in favor of methods with a higher level of objectivity (method of principal components; game methods; modeling methods).

3. Systematic updating of the list of indicators of the state of debt security, taking into account structural changes in the state's economy (including the replacement of the EMBI+Ukraine index indicator with the indicator of the sovereign credit rating of Ukraine, determined by the authoritative international rating agency Standard & Poor's).

4. Taking into account the non-linearity of economic processes, the application of the multiplicative form of the integral indicator of the state of financial security (5.6) instead of the additive form, among the shortcomings of which the significance of the integral indicator under the condition of zero data of individual indicators is highlighted, as well as the compensation of the value of the integral index for certain indicators at the expense of others:

$$FS_j = \prod_{i=1}^n y_{ij}^{a_i}, F, \text{ where } \sum_{i=1}^n a_i = 1 \text{ and } a_i \geq 1. \tag{5.6}$$

The region is one of the structural components, which is allocated according to the object of protection in the structure of financial security. The term "financial security of the region" is considered as the conditions for the financial development of a specific region within the state, under which internal and external threats do not lead to negative processes in a complex system

and do not prevent the creation of favorable financial conditions for the sustainable development of the region.

Therefore, in the process of monitoring the financial security of the region, it is necessary to calculate a certain complex indicator, the value of which will indicate the level of financial stability in the region, the investment climate, entrepreneurial activity and the standard of living of the population.

Ensuring the financial stability of Ukraine's regions is an important element of guaranteeing the overall financial stability of the state. This connection arises as a result of decentralization reforms aimed at creating effective local self-government to provide affordable and high-quality public services, establishing institutions of civic participation, creating a safe environment for residents, as well as coordinating the interests of local communities and the central government. Consequently, the quality of the performance of their functions by local government structures has a great impact on local tax policy, the formation of local budget revenues, the provision of insurance and banking services, the investment climate in the region and the standard of living of the population. These circumstances substantiate the need for a systematic and operational analysis of the financial stability of the regions of Ukraine in order to determine the strengths and weaknesses of the current state, diagnose opportunities and potential threats.

Methodological approaches [20] do not provide for a regional section of the assessment. It is possible to adapt the methodology for calculating the level of financial security of the state to the specifics of the regions, however, most indicators are based on statistical information at the state level and, accordingly, cannot highlight the specifics of regional development.

In order to assess the security level of the financial stability of the regions of Ukraine, their further analysis and comparison, as well as to identify the main problems, opportunities and possible threats, a methodical approach to monitoring the security level of the financial stability of the regions is proposed. This approach differs from those currently used, as it provides an opportunity to quickly assess the state of financial stability of individual regions of Ukraine and to identify specific threats and reserves specific to each region. This information can be used for further measures to increase the financial stability of specific regions.

At the first stage of the proposed methodical approach to the analysis of the financial security of the region, the category "financial security of the region" is decomposed into separate interconnected subsystems: financial security of the community of the region; economic entities of the region and their entrepreneurial activity; sectoral financial security of the region; security by the level of financial autonomy.

At the second stage, the list of quantitative indicators in the subsystems of the security level of financial stability of the region, which are interconnected with the state of financial security of the state, is formed. These indicators signal the degree of threats, are characterized by sensitivity to changes in the financial situation in the region, and can be used in the decision-making process in the field of financial policy.

The formed list of indicators must meet the following criteria: be scientifically based and be characterized by the availability of statistical data for the operational analysis of the financial

security of the region. Let's also note that the complex of selected quantitative indicators should be characterized by suitability for mathematical and other types of analysis, coverage of changes in a phenomenon or process over time, and unambiguous interpretation.

The selected indicators should be checked for multicollinearity, accordingly, indicators with a strong connection according to the Chaddock scale should be excluded from the system of indicators. In addition, we have to prove that the set of selected indicators are interconnected with the state of financial security of the state, which will confirm the hypothesis that the formed data matrix of the identified indicators can be used as input information in the process of calculating the integral indicator of the state of financial security of the region.

Formation of a set of indicators of the state of financial security of the region took place taking into account the principles of reliability, representativeness and information availability.

So, 22 financial indicators are selected, which are calculated by region and systematically published in the reports of the Ministry, which were previously checked for the presence of correlations. It has been verified that they are not in direct functional dependence. Each the selected indicators provides important information about the state of the financial security of the region, therefore, their comprehensive application is proposed for a comprehensive analysis.

A hypothesis is put forward, according to which the totality of these indicators objectively characterizes the state of financial security of the region, as well as specific problems and opportunities.

To prove or disprove this hypothesis, the basic ideas of the polynomial algorithm for the extrapolation of parameters of stochastic systems [31] were applied, on the basis of which a polynomial power correlation-regression model was developed for assessing the financial security of the region of Ukraine according to formula (5.7):

$$y_x^{(n,N)}(1, i) = M[X(i)] + \sum_{j=1}^n \sum_{w=1}^N (x^w(j) - M[X^w(j)]) S_{(j-1)N+w}^{(nN)}((i-1)N+1), \quad (5.7)$$

where $y_x^{(n,N)}(1, i)$ – state of the financial security of the region (realization at a point and a random sequence, provided that n elements are used with the highest order of stochastic connections N); $M[X(i)]$ – mathematical expectation of the state of financial security of the region; $x^w(j)$ – empirical values of indicators of the state of financial security of the region; $M[X^w(j)]$ – mathematical expectation of indicators of the state of financial security of the region; $S_{(j-1)N+w}^{(nN)}((i-1)N+1)$ – weighting factors [31].

Table 5.12 presents the calculated values of the state of financial security, calculated using the obtained polynomial correlation-regression model ($m_x^{(k,N)}(1, i)$), as well as the amount of error.

The determined values of the safety level of financial stability based on the values of 22 indicators, which are determined by region, differ insignificantly from the empirical values (the average level of error is 0.18 %), which justifies the statement about the relative accuracy of the forecasts made using this model and proves the declared hypothesis, that the set of selected indicators can objectively characterize the security state of the financial stability of the region and sufficiently accurately signal the presence of specific problems and opportunities of a specific region of the state.

● **Table 5.12** Results of approbation of a methodical approach to monitoring the level of financial security using a polynomial correlation-regression model

Years	State of financial security (according to the classical method), %	State of financial security (calculated according to the obtained model), %	Absolute error	Relative error, %
y		$y_x^{(n,N)}(\mathbf{1}, i)$		
2014	36.536	36.584	0.048	0.13
2015	35.847	35.761	-0.086	-0.24
2016	38.745	38.666	-0.079	-0.20
2017	40.023	40.081	0.058	0.14
2018	45.746	45.675	-0.071	-0.16
2019	42.669	42.575	-0.094	-0.22
2020	40.179	40.211	0.032	0.08
2021	41.123	41.198	0.075	0.18
2022	30.007	30.567	0.560	1.87
Average value of error				0.18

Note: calculated by the authors

At the second stage of applying the methodical approach to monitoring the security state of the financial stability of the region, the absolute values of the indicators by region were calculated and the data matrix $X = \{x_{ij}\}$ was built, where x_{ij} – the value of the j -th indicators for the i -th region of the state; $i = \overline{1, 22}$; $j = \overline{1, 24}$.

At the third stage of the application of the methodical approach to monitoring the security state of the financial stability of the region, the indicators are standardized in the financial security subsystems of the region. Normalization of indicators is proposed to be carried out using the method – relative to the range of variation (5.8), because it is this method that allows taking into account the difference in indicators in a certain period of the study.

$$C: y_{ij} = \frac{x_{ij} - x_{\min}}{x_{\max} - x_{\min}}; B: y_{ij} = \frac{x_{\max} - x_{ij}}{x_{\max} - x_{\min}}. \quad (5.8)$$

Matrix distribution $X = \{x_{ij}\}$, where x_{ij} – the value of j -th indicators for the i -th area; into groups is as follows: indicators characterizing the security level of financial stability of the population of the region have been added to the 1st group of indicators (matrix $X_{PR} = \{x_{ij}\}$). To the second – indicators that signal the level of financial security of economic entities and their entrepreneurial activity (matrix $X_{EE} = \{x_{ij}\}$). To the third – indicators characterizing the level of industry financial security of the region (matrix $X_{RS} = \{x_{ij}\}$). To the fourth – indicators of regional financial security according to the level of financial autonomy (matrix $X_{RS} = \{x_{ij}\}$).

At the fourth stage of applying the methodical approach to monitoring the security state of the financial stability of the region, weighting indicators were determined for the indicators of specific financial security subsystems of the region.

At the fifth stage of applying the methodical approach to monitoring the security state of the financial stability of the region, indicators were summarized into integral indexes of the state of regional financial security in terms of its subsystems, and regions were ranked according to the obtained values. The complexity of this stage is explained by a significant number of options for calculating the integral indicator, as well as disparities in the development of the regions of Ukraine.

At the sixth stage of the methodical approach, the integral value of the state of financial security by region and research period was determined, the regions were clustered according to the calculated values (**Table 5.13**).

● **Table 5.13** Clustering of regions of Ukraine by ranges of values of financial security of regions of Ukraine

Range	0.000–0.381	0.382–0.499	0.500–0.618	0.619–1.000
Security situation of the region	Critical	Dangerous	Satisfactory	High
Regions	Donetsk, Luhansk	Volyn, Zaporizhzhia, Zhytomyr, Mykolaiv, Zakarpattia, Kirovohrad, Chernivtsi, Rivne, Khmelnytskyi, Sumy, Ternopil, Kherson, Chernihiv, Kharkiv	Vinnitsia, Ivano-Frankivsk, Lviv, Odesa, Cherkasy	Dnipro, Kyiv, Poltava

Note: presented by the authors

Cluster analysis is a key tool for the typology of objects, the purpose of which is to divide objects into relatively homogeneous groups, taking into account the analysis of indicators that objectively characterize these objects.

In the process of calculating the integral indicator, the application of the additive model leads to the fact that there is a possibility of compensation for the deterioration of the safety level of one subsystem due to the increase in the safety level of another partial assessment. In order to prevent such a situation, the integral indicator, in our opinion, should be determined by the formula of the geometric mean (5.9):

$$FS_{ij} = \sqrt[4]{E_{1i} \cdot E_{2i} \cdot E_{3i} \cdot E_{4i}} = \sqrt[4]{\prod E_{ij}}, \tag{5.9}$$

where FS_{ij} – an integral indicator of financial security of the i -th region of Ukraine; x_{1i} , x_{2i} , x_{3i} , x_{4i} – partial coefficients.

The analysis results obtained by formula (5.9) may turn out to be incorrect, taking into account the theoretical possibility of zero values of x_{1i} , x_{2i} , x_{3i} , x_{4i} . Accordingly, let's apply the modified formula (5.10):

$$FS_{ij} = \sqrt{\prod(1 + E_{ij})} - 1. \tag{5.10}$$

As a result, a taxonomic integral value of the security state of the financial stability of the regions of Ukraine was obtained for periods in the interval from 0 to 1. Interpreting the value of this indicator, let's pay attention to the fact that high values of the indicator characterize a high level of security state of a certain region, and low values signal its critical state. The integral indicator of the security state of the financial stability of the regions of Ukraine is the result of collapsing the partial indicators into a complex index for a certain area.

The highest security level of financial stability of regions in 2022 was recorded in the following regions: Kyiv, Dnipro, Poltava, and the lowest – in Donetsk and Luhansk regions.

At the last stage of the proposed methodological approach, a comparison of the security state of the financial stability of the regions takes place, specific problematic aspects and opportunities of a certain region are highlighted.

The heterogeneity of the security level of financial stability of the regions of Ukraine is caused by the influence of economic, political, social and geographical factors.

CONCLUSIONS

Considering that the methodical approach to calculating the level of economic security of Ukraine, proposed for use in order No. 1277 dated October 29, 2013, does not provide for a regional assessment, a methodical approach to monitoring the security state of the financial stability of regions is proposed.

The given methodical approach includes the following sequence of actions: division of the component "financial security of the region" into subcomponents; creating a list of indicators for each financial security subsystem of the region; normalization of these indicators within the subsystem, determination of their importance for each separate subsystem of financial security of the region; generalization of indicators into complex indicators for assessing the state of financial security of the region in the context of various subsystems; ranking of regions according to the obtained values; calculation of the integral indicator of the state of financial security for individual regions and research periods, as well as grouping of regions based on the results obtained; comparing the state of financial security of regions based on the calculated values of the integral indicator of the state of financial security and highlighting specific aspects that are specific to each region.

A list of 22 indicators of the state of financial security of regions has been formed, which meets the following criteria: it is scientifically based, characterized by the availability of statistical data and suitability for mathematical and other types of analysis, highlighting the change of a phenomenon or process over time, unambiguous interpretation.

It is proved that the selected indicators of the state of financial security of the regions are not strongly related according to the Chaddock scale, and are also interconnected with the state of financial security of the state, which generally confirms the hypothesis that the formed matrix of data of the identified indicators can characterize the state of financial security of the region, testify

to specific problems and special opportunities in the region, and accordingly, be used as input information in the process of calculating the integral indicator of the financial security of the region.

On the basis of the proposed methodology for assessing the state of financial security of regions, integral indicators of the state of financial security of regions of Ukraine were calculated, which are actually the result of collapsing indicators by subsystems into a system index for a certain region, high values of which characterize a relatively stable value of financial security of a certain region, and low values signal its dangerous or critical condition. The regions of Ukraine were clustered according to the ranges of the financial security of the regions, according to the results of which the regions were divided into 4 groups: with a critical state of financial security of the region (0.000–0.381) (Luhansk, Donetsk), a dangerous state (0.382–0.499), a satisfactory state (0.500–0.618) and conditionally high (0.619–1.000) (Dnipro, Kyiv, Poltava).

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Akinleye, S. O., Dauda, R. O. S., Iwegbu, O., Popogbe, O. O. (2023). Impact of COVID-19 pandemic on financial health and food security in Nigeria: A survey-based analysis. *Journal of Public Affairs*, 23 (2). doi: <https://doi.org/10.1002/pa.2859>
2. Datsenko, G., Kudyрко, O., Krupelnytska, I., Maister, L., Kopchikova, I., Hladii, I. (2023). Application of the hierarchy analysis method to build a strategic map of the financial security of enterprises. *Financial and Credit Activity Problems of Theory and Practice*, 3 (50), 164–173. doi: <https://doi.org/10.55643/fcapt.3.50.2023.4013>
3. Davydenko, N., Bilyak, Y., Nehoda, Y., Shevchenko, N. (2020). Financial security for the agrarian sector of Ukraine. *Economic Science for Rural Development 2020*. doi: <https://doi.org/10.22616/esrd.2020.53.007>
4. Garškaitė-Milvydienė, K., Maknickienė, N., Tvaronavičienė, M. (2023). Insights into attitudes towards financial innovations by its users. *Polish Journal of Management Studies*, 27 (2), 106–119.
5. Hossain, Md. J., Jahan, U. N., Rifat, R. H., Rasel, A. A., Rahman, M. A. (2023). Classifying Cyberattacks on Financial Organizations Based on Publicly Available Deep Web Dataset. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 108–166. doi: <https://doi.org/10.1109/cymaen57228.2023.10050921>

6. Kovalenko, V., Slatvinska, M., Sheludko, S., Makukha, S., Valihura, V. (2023). The monetary component in ensuring the financial security of the state. *Financial and Credit Activity Problems of Theory and Practice*, 1 (48), 8–22. doi: <https://doi.org/10.55643/fcaptp.1.48.2023.3972>
7. Kryshatanovych, M., Shulyar, R., Svitlyk, M., Zorya, O., Fatiukha, N. (2023). Theoretical and methodological approaches to the formation of a model for increasing the efficiency of the system for ensuring the economic security of a banking institution. *Financial and Credit Activity Problems of Theory and Practice*, 2 (49), 56–64. doi: <https://doi.org/10.55643/fcaptp.2.49.2023.3994>
8. Knytska-Iliash, M. (2023). Assessment of the financial security of agriculture in Ukraine. *Agricultural and Resource Economics*, 9 (1), 5–27. doi: <https://doi.org/10.51599/are.2023.09.01.01>
9. Onyshchenko, S., Shchurov, I., Cherviak, A., Kivshyk, O. (2023). Methodical approach to assessing financial and credit institutions' economic security level. *Financial and Credit Activity Problems of Theory and Practice*, 2 (49), 65–78. doi: <https://doi.org/10.55643/fcaptp.2.49.2023.4037>
10. Panda, P. (2023). Innovative Financial Instruments and Investors' Interest in Indian Securities Markets. *Asia-Pacific Financial Markets*, 30 (1). doi: <https://doi.org/10.1007/s10690-023-09403-0>
11. Poltorak, A., Khrystenko, O., Sukhorukova, A., Moroz, T., Sharin, O. (2022). Development of an integrated approach to assessing the impact of innovative development on the level of financial security of households. *Eastern-European Journal of Enterprise Technologies*, 1 (13 (115)), 103–112. doi: <https://doi.org/10.15587/1729-4061.2022.253062>
12. Reshetnikova, N. N., Gornostaeva, Z. V., Chernysheva, Y. S., Kushnareva, I. V., Alekhina, E. S. (2023). The Global Financial Security and Financing for Sustainable Development Interaction: The Role of the ESG Factors. *Environmental Footprints and Eco-Design of Products and Processes*, 521–529. doi: https://doi.org/10.1007/978-3-031-28457-1_53
13. Salkić, H., Omerović, A., Salkić, A., Kvasina, M. (2023). Enhancing Economic Management with Information Technology: Insights from Covid-19 in Bosnia and Herzegovina. *Economics*. doi: <https://doi.org/10.2478/eoik-2023-0048>
14. Sirenko, N., Atamanyuk, I., Volosyuk, Y., Poltorak, A., Melnyk, O., Fenenko, P. (2020). Paradigm Changes that Strengthen the Financial Security of the State through FINTECH Development. 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). doi: <https://doi.org/10.1109/dessert50317.2020.9125026>
15. Vyhovska, N., Voronenko, I., Konovalenko, A., Dovgaliuk, V., Lytvynchuk, I. (2023). Cyber Security of the System of Electronic Payment of the National Bank of Ukraine. *Economic Affairs*, 68, 881–886. doi: <https://doi.org/10.46852/0424-2513.2s.2023.34>
16. Xie, X., Osińska, M., Szczepaniak, M. (2023). Do young generations save for retirement? Ensuring financial security of Gen Z and Gen Y. *Journal of Policy Modeling*, 45 (3), 644–668. doi: <https://doi.org/10.1016/j.jpolmod.2023.05.003>

17. Yekimov, S., Prodius, O., Chelombitko, T., Poltorak, A., Sirenko, N., Dudnyk, A., Chernyak, V. (2022). Reengineering of agricultural production based on digital technologies. *IOP Conference Series: Earth and Environmental Science*, 981 (3), 032005. doi: <https://doi.org/10.1088/1755-1315/981/3/032005>
18. Yekimov, S., Purtov, V., Buriak, I., Kabachenko, D., Poltorak, A. (2021). Improving the efficiency of corporate management of agricultural enterprises. *Innovative Technologies in Environmental Engineering and Agroecosystems*, 262, 03001. doi: <https://doi.org/10.1051/e3sconf/202126203001>
19. Yekimov, S., Sarychev, V., Malyuga, N., Shkulipa, L., Poltorak, A. (2021). The role of the state in increasing labor productivity in agricultural enterprises of Ukraine. *Fundamental and Applied Research in Biology and Agriculture: Current Issues, Achievements and Innovations*, 254, 10002. doi: <https://doi.org/10.1051/e3sconf/202125410002>
20. Pro zatverdzhennia Metodychnykh rekomendatsii shchodo rozrakhunku rivnia ekonomichnoi bezpeky Ukrainy (2013). Nakaz Ministerstva ekonomichnoho rozvytku i torhivli Ukrainy No. 1277. 10.29.2013. Available at: <https://zakon.rada.gov.ua/rada/show/v1277731-13#Text>
21. Pro zatverdzhennia Serednostrokovoi stratehii upravlinnia derzhavnym borhom na 2021–2024 roky (2021). Postanova Kabinetu Ministriv Ukrainy No. 1291. 09.12.2021. Available at: <https://zakon.rada.gov.ua/laws/show/1291-2021-%D0%BF#Text>
22. Nkeki, C. I. (2018). Optimal investment risks and debt management with backup security in a financial crisis. *Journal of Computational and Applied Mathematics*, 338, 129–152. doi: <https://doi.org/10.1016/j.cam.2018.01.032>
23. Derzhavnyi borh ta harantovanyi derzhavoiu borh Ministerstvo Finansiv Ukrainy. Available at: https://mof.gov.ua/uk/derzhavnij-borg-ta-garantovaniy-derzhavju-borg_osn_inf
24. National Bank of Ukraine (2023). Indicators of the banking system. Available at: <https://bank.gov.ua/ua/statistic>
25. State Statistics Service of Ukraine. Available at: <https://www.ukrstat.gov.ua/>
26. Khalatur, S., Velychko, O., Oleksiuk, V., Kravchenko, M., Karamushka, D. (2023). Financial security as a component of ensuring innovative development of agricultural production. *Financial and Credit Activity Problems of Theory and Practice*, 3 (50), 341–356. doi: <https://doi.org/10.55643/fcaptop.3.50.2023.4050>
27. Poltorak, A., Potryvaieva, N., Kuzoma, V., Volosyuk, Y., Bobrovska, N. (2021). Development of doctrinal model for state financial security management and forecasting its level. *Eastern-European Journal of Enterprise Technologies*, 5 (13 (113)), 26–33. doi: <https://doi.org/10.15587/1729-4061.2021.243056>
28. Poltorak, A., Volosyuk, Y., Tyshchenko, S., Khrystencko, O., Rybachuk, V. (2023). Development of directions for improving the monitoring of the state economic security under conditions of global instability. *Eastern-European Journal of Enterprise Technologies*, 2 (13 (122)), 17–27. doi: <https://doi.org/10.15587/1729-4061.2023.275834>

29. Tong, E. (2024). Repercussions of the Russia–Ukraine war. *International Review of Economics & Finance*, 89, 366–390. doi: <https://doi.org/10.1016/j.iref.2023.07.064>
30. Kharazishvily, Yu. M. (2014). Methodological Approaches to Economic Security Evaluation. *Science and Science of Science*, 4, 44–58.
31. Atamanyuk I., Kondratenko Y., Shebanin V., Sirenko N., Poltorak A., Baryshevska I., Atamaniuk V. (2019). Forecasting of cereal crop harvest on the basis of an extrapolation canonical model of a vector random sequence. *Proceedings of 15th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. ICTERI Kherson, Ukraine, 2393*, 302–315.

CHAPTER 6

CURRENT ISSUES OF INNOVATIVE DEVELOPMENT AND EVOLUTION
OF THE CIRCULAR ECONOMY AT THE REGIONAL SCALE

ABSTRACT

The essence and features of the circular economy as an innovative component of the modern economy, which functions and develops on the basis of sustainable development, the deep reasons for its emergence, formation and transformation into a factor in the formation of a new paradigm of the global economy are considered. Being a mechanism for the implementation of the Global Goals of sustainable development, the concept of a closed cycle economy encourages highly developed countries and businesses to introduce innovations and define the development of a circular economy as a priority in their long-term strategies. Special attention is paid to the analysis of the evolution of the circular economy in the countries of the European Union, the problems and prospects of the development of the circular economy in Ukraine.

KEYWORDS

Linear economy model, sustainable development, innovative development, circular economy, innovative system, innovative infrastructure, evolution of the circular economy, business model of a closed cycle.

In recent decades, there has been a sharp increase in the negative anthropogenic impact of humanity on the natural environment both at the national and global levels. According to experts, further economic growth will inevitably lead to an increase in the use of natural resources and consumption waste. This, in turn, will further exacerbate environmental problems, such as loss of biodiversity, pollution of water, air and soil, depletion of resources, and will increasingly endanger the Earth's life support system. On the other hand, societal expectations are not being met due to issues such as high unemployment, poor working conditions, social vulnerability, the poverty trap, intergenerational injustice and widening inequality. Economic challenges such as supply risk, problematic ownership structures, deregulated markets, and imperfect incentive structures lead to increasingly frequent financial and economic instability for individual companies and the entire economy [1].

So, the model of the traditional linear economy, which functions according to the principles: "Take, Make, Waste (Dispose)" (extract, use, throw away (dispose); "raw materials – processing – waste"; "production – use – disposal" has already exhausted itself. It should be replaced by a new model of modern economic development, based on the rational consumption and restoration of resources and the minimization of negative human impact on the environment. This model has received the name closed-loop economy or circular economy (English closed-loop economy, circular economy). At the same time, society itself must change – from the choice of raw materials, product development methods and new service concepts to the widespread use of by-products of one industry as complete raw materials for another [2].

The circular economy emerges from the innovation economy, when breakthrough innovative technologies together with innovative business processes form closed cycles of processing, exchange and consumption.

Today, the path to a circular economy is being overcome by many countries of the world, according to researchers, 9 % of the world economy is circular. The analysis of trends in its development gives grounds for asserting that the share of the circular economy will continue to grow steadily. In some highly developed countries, the formation and development of the circular economy is becoming the main factor in achieving the goals of sustainable development. That is why the study of various aspects of the evolution of the circular economy is extremely relevant.

The study of the circular economy attracts considerable attention of many scientists. Among the researchers, it is worth noting the works of M. Geissdoerfer, P. Savaget, R. Merli, M. Preziosi, A. Acampora, A. Petit-Boix, S. Leipold, among the domestic ones – O. G. Melnyk., D. Bayura, M. O. Varfolomeeva, I. Ya. Zvarycha, D. Z. Nechitalo, S. M. Lyholat, L. V. Deineko, O. Sysoev, M. V. Rudy, K. V. Savitska The aim of research the peculiarities of the formation and evolution of the development of the circular economy in the regional dimension as a fundamental direction of the development of the modern global economy.

The basis of the economic growth of any country and the successful functioning of enterprises is the process of innovative development, which forms positive qualitative and quantitative changes in the production and economic system. At the same time, it is important to understand that in the new economy, accelerating the pace of economic development becomes one of the priority tasks at the same time as ensuring its sustainability.

Innovative development can be defined as a complex economic category that is associated with innovative changes and adaptation of enterprise management processes to the requirements of the external and internal environment [3].

In other words, innovative development represents changes aimed at updating and qualitatively increasing the efficiency of processes or products, which is accompanied by a transition to a new level of system organization [4].

Therefore, innovative sustainable development can be understood as an irreversible, directed, natural change in the economic situation, innovative and social infrastructure of the socio-economic system, as a result of which it moves to a qualitatively new progressive state.

Let's clarify that we do not apply the characteristic "fundamental" to the specified changes, since sustainable development implies, in our opinion, the "soft" nature of changes with smaller losses due to transformational changes in the market economic system.

At the same time, the innovative development of the enterprise, as an activity of the enterprise, is based on the constant search for new methods and means of satisfying consumer needs and increasing the efficiency of management; development, which involves the expansion of the boundaries of innovative activity and the introduction of innovations in all spheres of enterprise activity, the creation and practical use of innovations [5].

It is important to understand that innovative ideas emerge and transform ordinary economic projects into innovative development when different creative thoughts are combined into a single system supported by an institutional environment and innovative infrastructure. They are the ones who should ensure the integration between research and development, marketing and other components, for example, a large enterprise with structured scientific and research capital, or, for example, an innovative cluster of medium and small enterprises, when the circulation of innovative ideas can occur more chaotically, as, for example, by the modern method of open innovation. Chaoticity in this case also brings positive opportunities for generating unexpected innovative ideas and results.

The innovation system plays the role of an institutional basis for the innovative development of the national economy. Its functioning creates prerequisites for the transformation of ideas, new knowledge into innovation with their further implementation with the aim of obtaining an economic or any other effect. Within the innovation system, there is an interaction of all subjects directly or indirectly involved in the innovation process, and the effectiveness of its functioning is determined by the effectiveness of the interaction of all structural elements [6].

It is important that the national innovation system itself, on the one hand, is a process of interaction between various institutions involved in the process of production and commercialization of scientific knowledge within the state, and on the other hand, it is the result of this interaction. The determining factor of the effective functioning of the national innovation system is the degree of partnership in the "science-business-state" system, which combines technological, financial and organizational factors of generating and spreading innovations [7].

Modern innovative infrastructure is an important factor in the innovative development of the region. Thus, innovative infrastructure, in particular its most concentrated elements, forms the centers (poles) of the growth of entrepreneurial activity and the placement of science-intensive technologies. Therefore, the supporting frame of the industry is being built on the basis of such centers. At the same time, it is necessary to take into account that the development and implementation of innovations at enterprises has a twofold effect on the functioning of the industry of the region. On the one hand, the innovative activity of enterprises helps to increase their competitiveness both on the regional, national and international markets, and on the other hand, a large share of innovative products in a specific enterprise leads to a significant increase in the risks of entrepreneurial activity itself [8].

When considering the essence of the modern concept of economic development, first of all, it is necessary to consider the development of the scientific and technical revolution as a result

of scientific and technical discoveries, as a result of which society receives fundamentally new equipment and technologies that allow increasing labor productivity tens and hundreds of times [2].

At the same time, the modern paradigm of global development is the idea of sustainable development, which is shaped by the Sustainable Development Goals (SDGs) of the United Nations and relevant scientific theories. Importantly, sustainable development implies system-driven development, when the concept of innovative activity also falls under the positive influence of the SDGs.

Thus, innovations in the European Union shape markets, transform the economy, stimulate gradual changes in the quality of public services and are indispensable for achieving the main goals of double "green" and digital transit [9].

As stated in the Decree of the President of Ukraine "On the Goals of Sustainable Development of Ukraine for the period until 2030", the SDG of Ukraine for the period until 2030 are guidelines for the development of projects of forecasting and program documents, projects of regulatory and legal acts in order to ensure the balance of economic, social and environmental dimensions sustainable development of Ukraine. SDG No. 9 is aimed at building sustainable infrastructure, promoting sustainable industrialization and stimulating innovation [10].

It should be noted that a new wave of innovation is on the horizon: deep technological innovation that is based on advanced science, technology and engineering, often combining advances in the physical, biological and digital spheres and with the potential to provide transformative solutions in the face of global challenges. In particular, the deep technological innovations emerging from the growing cohort of innovative start-ups in the EU have the potential to drive innovation in the economy and society. This, in turn, can change the business landscape of the EU and related markets and help in solving the most pressing societal problems, in particular by achieving the UN Sustainable Development Goals [9].

Europe is also one of the fastest growing private equity investment regions. Between 2016 and 2020, it experienced faster growth than China and the US, albeit from a lower base. It is important to pay attention to the following:

1. EU companies are world leaders in high-value environmental patents and environmental patents in energy-intensive industries.
2. Europe's powerful industrial base is characterized by an increasingly dynamic startup ecosystem. Deep technological innovation results in physical products, not pure software services.
3. Deep technological innovations are aimed at solving key societal problems. This is particularly evident in the EU's position in wind energy: bold policy decisions such as climate change interventions and environmental protection, combined with close cooperation between the public and private sectors, the strengths of the single market have created the conditions for European companies to thrive in the sectors of the future, which are based on deep technologies [9].

At the same time, it is advisable to take into account that the advantages of borrowing new knowledge from abroad for Ukraine are obtaining technologies that have been used in practice and meet world standards. This contributes to the formation of technological cycles together with foreign enterprises, the acquisition of experience in the implementation of marketing approaches

in the field of innovation. However, it is important for Ukraine to prevent the receipt of morally outdated innovations, as well as the deepening of dependence on technology supplier countries [11].

Recently, the economy of Ukraine has suffered significant losses as a result of the military aggression of the Russian Federation against our country. In particular, industrialized regions suffered significant destruction, leading to a significant loss of both productive capital and the destruction of value chains and related commercial linkages.

The recovery of Ukraine's economy, in terms of its integration into the European economic system, should be based on the activation of innovative development processes. Accordingly, in the post-war period, innovation policy in Ukraine should implement system tools for appropriate modernization of the economy and activation of internal and external factors of the country's socio-economic development in interaction with the European innovation ecosystem [12].

It is important to note that the process of innovative development at the micro level may differ from enterprise to enterprise, which is influenced, among other things, by the sector of activity or the size of the company. For example, the structure of small and medium-sized enterprises is lean and flexible compared to large companies and can be considered more organic than mechanical. Such businesses have a highly skilled workforce, few hierarchical levels, few if any divisions, and proximity to customers. This means that from the point of view of the innovation development process, they have the potential to manage knowledge faster than large companies in order to create new products [13].

Small and medium-sized technology companies do not innovate systematically, but intuitively and focus on the ideas of their founders and, mainly, on satisfying customer and market needs. Small and medium-sized technological companies in the innovation process are characterized by high adaptability and flexibility in their management and innovation methods, even though they have few resources to invest in research and development [13].

Evaluation of innovative projects should be optimally balanced in modern conditions. Making an appropriate decision regarding their feasibility requires the use of a comprehensive approach and the development of new tools for evaluating the effectiveness of innovative projects using IT technologies [14].

When considering the requirements for the content of the concept of evaluation of various aspects of innovative activity, as a rule, the influence of a set of factors on it is taken into account, such as, for example, a set of indicators in the following areas: technological, economic, political-legal and organizational-management [1, 13].

At the same time, it is advisable to consider innovative and investment activities as a single process, the separate implementation of the components of which is either ineffective or impossible [15].

As a rule, the economic effect is understood as the result that leads to a quantitative increase in the company's resources, in particular labor, material or natural resources. This effect is estimated on the basis of indicators of profitability from the implementation of innovative products, the introduction of new technologies into production, as well as at the expense of profit from the introduction of inventions and industrial samples into the production process. At the same time, an increase in the share of information technologies involved in the production process, an increase

in the level of automation and robotization of production, as well as an increase in the number of know-how developed within the enterprise form the basis for evaluating the scientific and technical effect. When considering social impact, it is important to understand that social impact is the result of the degree to which society's needs are met. This effect cannot be quantified and valued, so its measurement is mostly limited to qualitative methods based on consumer judgments. The resource effect shows the change in the volume of production and consumption of a certain type of resources depending on the impact of the corresponding innovative component. It is manifested in the release of resources at the enterprise [1, 16].

In addition, the assessment of the environmental effect, which reflects the impact of the innovative activity of the enterprise on the environment and is characterized by indicators of reducing environmental pollution, reducing the energy intensity of production, improving the environmental friendliness of products, etc., is becoming more and more relevant today for the assessment of innovative activity in the modern economy [1].

This relevance is confirmed by the formation of the emergent content of economic models of highly developed market economies, in particular, the active development of the circular economy.

The birth and formation of the circular economy began in the 70s of the 20th century, although the term "circular economy" appeared for the first time only in 1990 [17].

In wide usage, the term "circular economy" was preceded by the similar term "green economy", which entered wide circulation during the global economic crisis of 2008–2009. In 2009, the United Nations Environment Program published the report "Global Green New Deal", which considered the goals, tasks, elements, incentives and directions of domestic policy aimed at the development of the green economy. The priorities of the green economy were determined, on the one hand, by maintaining and restoring natural capital; use of renewable energy and low-carbon technologies for fossil fuels; increasing the efficiency of resource and energy use; formation of responsible behavior of city residents; transition to low-carbon mobility; and on the other hand, creating new jobs and improving social justice [18].

In the last decade, special attention is paid to the research of the circular economy itself as a new model of economic development, based on the implementation of closed cycles in the processes of production, circulation and consumption, which allows creating additional value. The generally recognized basic principles of its functioning are the 3R principles recorded in many international documents: Reduce (reduction of resource consumption), Reuse (reuse of manufactured products), Recycle (processing of by-products and waste)). With the development of the circular economy, more detailed interpretations of the principles of the 6R circular economy began to be used: Reduce, Reuse, Repair, Refurbish, Recycle, Recover [19].

Over time, the principles of the circular economy were transformed into 9R [20]:

1. Refuse: rejection of excessive use of resources by refusing to use components that do not affect product quality or are not environmentally friendly at each stage of the product's life cycle.
2. Reduce: reducing the use of resources by implementing technical and organizational solutions to increase the efficiency of production, sales and responsible consumption of products.

3. Reuse: the process of using a product that has lost its value for one user, but represents value for another user and can be used for the purpose of generating additional profit and reducing the burden on the environment.

4. Repair: Is the process of extending the life of the product through repair and additional maintenance.

5. Refurbish: Updating an old product in order to match the functionality and appearance to modern customer requirements.

6. Remanufacture: production of new products from elements of the old one.

7. Repurpose: using the product for other purposes.

8. Recycle: recycling and secondary use of materials.

9. Recover: production of energy from materials.

It should be noted that in 2018, the principles of the closed-loop economy were expanded to 10R by the World Economic Forum (**Fig. 6.1**).

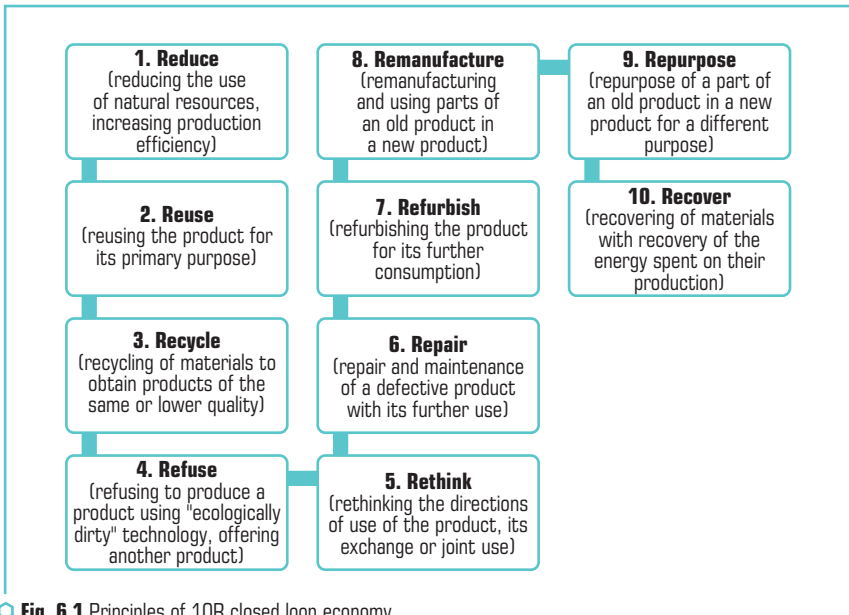


Fig. 6.1 Principles of 10R closed loop economy
Source: [21]

In general, the evolutionary development of circular can be divided into three stages [19]:

1. At the first stage (1970–1990), work with waste took center stage. In European countries and the USA, a number of environmental legislation was adopted. The greatest interest at this time is the concept of 3R. The principle known as "polluter pays" is emerging. At the same time, due to

the insufficient development of ecological culture at that time, the approach is gaining popularity, according to which the territory of less developed countries begins to be used for the burial of waste and/or its processing.

2. In the second stage (1990–2010) – the stage of the environmental efficiency strategy – the introduction of environmental payments (charges for pollution) had a significant impact on the development of the circular economy. In the early 2000s, a number of environmental problems were recognized as global (in particular, the destruction of the ozone layer, global warming). During this period, the scientific community is actively developing possible ways of waste-free industrial production.

3. In the third stage (approximately from 2010 to the present) – the stage of maximum conservation in the era of resource depletion – the threat to the survival of humanity due to the reduction and gradual disappearance of the necessary natural resources, the growth of the global population and the amount of waste is recognized as the central problem. Producers of goods and services are offered to develop taking into account three key principles: green innovation, alternative sources, and a change in the industrial paradigm.

Today, the main activities within the circular economy include reuse, repair, renewal and restoration (Recover), recycling of existing materials and products, as well as preventive actions to reduce the amount of waste. The main idea is that what was previously considered "waste" can turn into a valuable resource [22]. This reduces the negative impact on the environment and allows efficient use of limited natural resources, as used materials and waste become raw materials for the economy again. New sales markets are emerging, new products are being developed, competitive business models are being created, manufacturers are preparing for the challenges that the future will bring them.

The implementation mechanism of one of the Global Sustainable Development Goals (SDGs), approved at the UN Summit in September 2015, namely: "Responsible consumption and production", is recognized as "...the introduction of a circular economy model, primarily by focusing on energy saving, regenerative, environmentally friendly production and consumption" [23]. It is important to note that the circular economy concept not only corresponds to all 17 UN Sustainable Development Goals, but also encourages countries and businesses to innovate. And today, most EU countries, the USA, China, Japan, South Korea and other countries have prioritized the development of the circular economy in their long-term strategies. This can be explained by the fact that the use of circular production, unlike linear production, allows optimal disposal of waste, reducing the scarcity of resources, especially natural ones, reducing the negative impact on the environment and achieving competitive advantages in international markets due to innovations [18].

The circular economy strategy as an integral part of the modern economy is implemented by 44 % of companies from the top 100 Fortune Global list, and around 500 multinational companies in the world. According to The Circularity Gap report, presented annually at the World Economic Forum in Davos, in 2018, 9 % of materials in the global economy were reused. The leaders in implementing the principles of the circular economy are the production of goods of daily

demand (FMCG – "Fast Moving Consumer Goods") and the automobile industry [24]. Other industries do not yet practice the closed loop so widely.

To date, the most significant results from the point of view of the transition to a circular economy are demonstrated by the countries of the European Union, where the European Resource Efficiency Platform, which unites EU countries, is designed to ensure the transition to a circular economy, strengthen global competitiveness, promote sustainable economic growth and create new jobs [25].

In the package of Directives in the field of waste management, adopted by the EU Commission in December 2015, the EU Action Plan was approved, which provides for specific measures for the development of the circular economy, covering the entire cycle: from production and consumption to waste management and the market for secondary raw materials, and also defines time limits for performing the described actions. The proposed measures involve "closing" the life cycle of the product through recycling and reuse, which will benefit both the environment and the economy [19]. It should be noted that on March 11, 2020, the European Commission adopted a new special plan – the Circular Economy Action Plan, which is also the basis of the Strategy for the Development of the "Green" Economy in the EU and provides for a number of innovations and changes, the implementation of which will make it possible to transform Europe into a climate-friendly one by 2050 – a neutral continent, will contribute to economic growth, increase in well-being and standard of living of citizens, greening of the economy and protection of the environment. According to the plan, it is expected to double the level of reuse of resources in the next ten years and to create an additional 700,000 new jobs [26, 27].

Separate (main) areas of circular economy development in EU countries are [28]:

- 1) **marine litter processing**, which can ensure a reduction of marine litter from 13 % in 2020 to 27 % in 2030;
- 2) **use of construction and demolition waste** by implementing a mechanism for assessing the environmental performance of new buildings;
- 3) **reduction of food waste** in production, retail trade, food services and households by at least 30 % by 2025;
- 4) **improving the management and processing of plastic waste**. It is assumed that by 2030, all plastic packaging should be recycled;
- 5) **promotion of the processing of the most important raw materials** within the framework of the raw materials initiative and the European innovative partnership for raw materials.

According to the calculations of the EU institutions, "the implementation of resource-efficient production technologies at all links of production chains will allow to reduce the industrial demand for raw materials by 17–24 % by 2030, the annual costs of enterprises – by 630 billion EUR" [25], and the transition to a circular economy will generally increase Europe's GDP by 17 % by 2030 [29].

In some countries of the European Union, models of circular economy development at the macroeconomic level are already being formed today. For example, the Netherlands is creating a circular economy due to innovations, Scotland – thanks to a special investment fund that finances

circular economy projects, and Finland was the first in the world to develop a national road map for the transition to a circular economy [18].

Factors related to averting a climate catastrophe, as well as the dependence of many countries on limited natural resources, and primarily energy, became the impetus for a new rethinking of the provisions regarding the circular economy. In these conditions, the creation of so-called durable products and the improvement of the efficiency of resource reuse in the industrial sector are of particular importance [18]. The very nature of the circular economy provides for the broad development of an innovative model of the economy. At the same time, "circularity becomes one of the forms of dynamic development of the socio-economic system at different levels of management" [30].

At the micro level, the principles of the circular economy are implemented with the help of various business models, strategies and tools.

In work [19], business models of the circular economy are divided into 2 groups:

The first group includes business models of reuse of resources due to repair, reconstruction, modernization, re-equipment of already operating enterprises.

The second group includes business models of materials processing. They envisage the creation of completely new factories that will be able to process waste after linear enterprises.

Today, various strategies, business models and approaches to the circular economy, which provide an opportunity to obtain additional sources of income, have become widely used in companies around the world. Among the main researchers [20, 24, 26, 31] single out the following:

1. Design of the future. It involves the production of goods in which traditional materials can be replaced by renewable or recycled ones. This optimizes the use of resources and reduces the amount of waste in the production process. For example, Adidas has developed running shoes made of 100 % recycled materials. In production, one type of material is used and no glue is used. After use, the shoes can be recycled to produce a new pair.

2. Design without waste. According to this strategy, product design takes into account the possibility of repair, restoration and reuse after the end of the service life.

3. Shared use and virtualization – the business models of Uber, BlaBlaCar, and Airbnb, already familiar to many, use this approach. Ukrainian examples include the Oh My Look! brand, which is transforming from a dress rental service to offering a subscription-based virtual wardrobe. Similar services work successfully in many countries of the world.

4. "Segmentation of flows" involves the separation between consumables and components of long-term use of products for the purpose of reuse or safe return to the biosphere.

5. "Goods as a service" strategy seeks to replace traditional models of selling goods with the implementation of services. Thus, the Rolls Royce concern with the "Power-by-the-Hour" service offers customers from the aviation industry, instead of buying aircraft engines, payment for their use based on a fixed rate for 1 hour of work. Due to the service approach, the life cycle of the engine increases by 25 %.

6. Reuse in production – when used products or components become part of new products. So, Canon takes back products at the end of their life cycle and uses the components in new

devices, without reducing the functional characteristics of the materials. And the Michelin group annually returns 17 million tons of used car tires to the production process. Thanks to R&D developments, they become a valuable material again.

7. Reuse in consumption involves the sale and purchase by companies of used functional goods at reduced prices. In Sweden, there is an entire Retuna supermarket, the range of which consists of second-hand items, from furniture to books. And most Kyivans know about the "Courage Bazaar" project, which promotes reuse.

8. Industrial symbiosis and recycling of production waste can also significantly increase business efficiency.

The project in the city of Kalundborg, Denmark, is considered the first example of symbiosis in the concept of circular economy. Participating companies were united there by the principle of interaction, when production waste of one business becomes a resource for another. At the same time, economic costs and CO₂ emissions are reduced. The consortium includes the largest oil refining company in Denmark, the pharmaceutical company Novo Nordisk, the municipal water and heat supply company for city residents, a waste management operator and other participants.

In Ukraine, there are also examples of effective use of resources in the production process. For example, the company "Myronivskiy Hliboprobukt" is building biogas complexes for processing waste from poultry farms and obtaining energy. Concern "Obolon" sells to agricultural companies by-products of beer production, which become fodder for animals. And in the "Silpo" chain of supermarkets, special heat recovery tanks from refrigeration equipment are installed to meet the need for hot water supply.

9. The term "**recycling**" is also a circular economy strategy. At the end of the product's life cycle, the materials are recycled in a safe way. For example, sports shoe manufacturer Nike launched the Nike Grind initiative almost 30 years ago. Old sneakers, collected all over the world, were used as a material for the manufacture of coverings for sports fields. Since its launch, about 28 million pairs of shoes have been recycled into sports surfaces.

10. Clean energy involves the use of energy from renewable sources to increase the stability of the cycle system and reduce dependence on changes in the cost of resources.

It should be noted that obtaining competitive advantages for business, according to experts, is also achieved by changing the rate of resource consumption and applying a complex of cyclical principles "3R", "6R", "9R".

So, as the experience of developed countries, primarily European, shows, the circular economy offers a more rational approach to the use of resources in general and waste management, in particular.

The situation in Ukraine in this regard is much more modest, since the circular economy in our country is just starting to develop, and the topic of its widespread implementation remains open according to some estimates [31]. Despite the fact that there are already the first significant steps on the way to the transition to a circular type of economy, which are based on the experience

of Europe [17, 32, 33], on the one hand, there are many issues that require practical implementation both at the state level and at the level of business, and on the other hand, very few steps have been taken on the way to a circular economy, although there is an understanding of the need for reforms at different levels (government, business and the public) [4].

In practice, the implementation of circular economy principles faces significant obstacles. The main factors that negatively affect the development of the circular economy in our country are [28, 21, 31]:

- 1) extremely high prices for transporting raw materials for repeated processing;
- 2) imperfect logistics infrastructure, mostly poor-quality roads;
- 3) the market of secondary raw materials is opaque, as more than 50 % is in the shadows. At the same time, the market for recycling and waste-free technologies is at an early stage of development;
- 4) absence of tariffs for processing of secondary resources;
- 5) low level of environmental tax and other eco-payments, which, on the one hand, leaves support for measures aimed at building a circular economy, and on the other hand, does not stimulate manufacturers to implement closed-loop technologies;
- 6) practice of public procurement, where the main criterion for choosing a supplier is usually the cheapest offer. At the same time, other criteria are not taken into account, such as energy efficiency, chemical safety, resource conservation, prevention of environmental pollution, reduction of the negative impact of climate change, and reduction of waste volumes. Products that are better in terms of environmental friendliness and energy efficiency usually do not have the opportunity to beat cheaper products made with the help of "ecologically dirty" technologies;
- 7) uncertainty with tariff policy in green energy.

As a result, the Ukrainian economy is characterized by low efficiency of resource use, has a very low share of recovery and reuse of waste, and in this respect lags far behind developed European countries.

Fig. 6.2 presents statistical data on waste management in the EU and Ukraine. The given data show that both the EU countries and Ukraine still lack technologies to prevent the generation of waste. At the same time, if in Ukraine more than 94 % of waste is buried or burned, then in the EU – only one fourth (25.3 %). Accordingly, in the EU, preparation for reuse and recycling make up almost half (48.1 %) of waste, in Ukraine – only about 6 %. In addition, for 265.6 % of waste in EU countries, another type of disposal is used, which includes energy recovery.

According to experts, the transition from a linear model of the economy to a circular one will contribute to the improvement of the country's economic climate, the creation of new market niches (remanufacturing, engineering, processing, service), an influx of investments, as well as new business models. Ukraine can become an Eastern European hub in this new reality by joining its construction at an early stage. But in order to reach this qualitatively new level of resource efficiency, technological innovations and changes in behavior patterns, large-scale investments and special packages of state incentives will be needed [25].

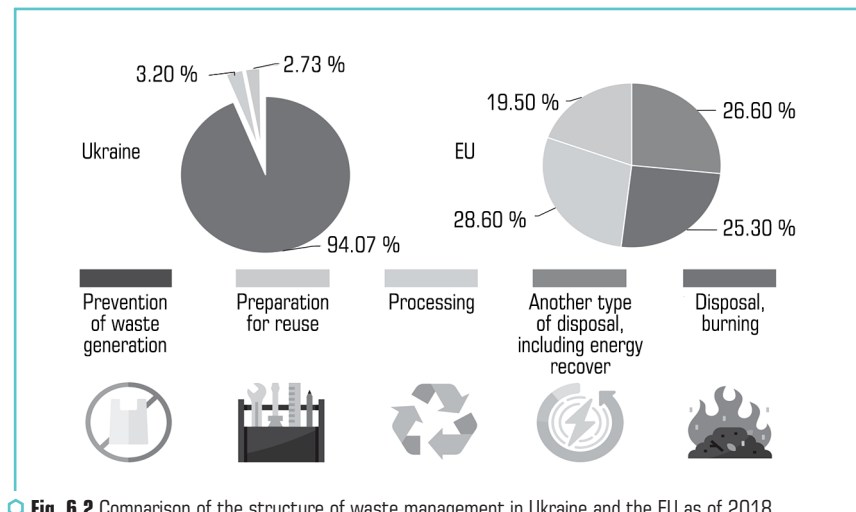


Fig. 6.2 Comparison of the structure of waste management in Ukraine and the EU as of 2018
 Source: [19]

The first step in the field of state support for the transition to the principles of a circular economy was the approval by the Cabinet of Ministers of Ukraine in November 2017 within the framework of the Association Agreement between Ukraine and the EU of the National Waste Management Strategy in Ukraine until 2030.

The implementation of the principles of the circular economy will also be facilitated by the gradual harmonization of our country's legislation with European legislation within the framework of EU membership. In this context, the Law of Ukraine "On Waste Management" was adopted in June 2022, which is an important step on the way to the functioning of extended producer responsibility (EPR) systems, which should stimulate producers to implement closed-loop technologies.

Currently, the Government of Ukraine is considering the issue of forming a Ukrainian green course based on the strategy of the European Green Course (European Green Deal), the basis of which is, as already mentioned above, the Circular Economy Action Plan.

The main program documents on the circular economy in Ukraine are as follows:

- national waste management strategy until 2030;
- national Waste Management Plan until 2030, adopted by the CMU on February 20, 2019;
- national waste management plan until 2030;
- strategy of the state environmental policy of Ukraine for the period until 2030;
- concept of implementation of state policy in the field of climate change for the period up to 2030 and its implementation plan;
- low-carbon development strategy of Ukraine until 2050, etc. [1, 4].

These documents provide [21]:

- implementation in Ukraine of the best European practices in the field of handling various types of waste (industrial, solid household, agricultural waste, construction, hazardous and other types of waste);
- construction of an innovative waste management model;
- specific tasks and measures that will allow Ukraine to move to a new model of waste management, to a closed cycle economy, which is used by leading European countries by 2030;
- measures to reduce water and air pollution through the introduction of environmental norms and standards;
- transition of Ukraine's economy to a low-carbon development model, which consists in the transition to renewable energy sources and mainly in reducing emissions of greenhouse gases into the environment;
- implementation of the concept of ecological production in Ukraine through the use of "green" (ecological) technologies.

Despite the large number of adopted program documents, Ukraine has not yet formed a coherent system of support for the development of the circular economy. Concrete, rapid changes are needed that will contribute to the formation of a closed-loop economy.

At the macro level, in addition to the goals, tasks and specific measures defined by the set of program documents, the state must develop effective mechanisms for their implementation. The first direction of effective state regulation of the development of the circular economy should be the formation and harmonization with European legislation of the legislative and regulatory framework, which would encourage producers of goods and services to use effective innovative technologies of the closed cycle.

In our opinion, one of the key mechanisms for stimulating the introduction of closed-loop technologies is the transformation of the public procurement system in accordance with the needs of the development of the circular economy. The main element of the procurement system (this will be especially relevant in the conditions of the post-war reconstruction of the economic and social infrastructure) should be the unconditional (unquestionable) consideration of the criteria of environmental friendliness and energy efficiency of the purchased products at all levels: from state to local.

The third direction of state support for the development of the circular economy should be partial or full financing of waste processing and disposal projects at the state and regional levels.

All this will allow enterprises to more actively transition to modern business models of the circular economy and closed-loop technologies. By developing and further implementing innovative business models, it will be possible to guarantee that natural resources will be preserved.

Current areas of circular economy development in Ukraine are:

- development of green energy (alternative energy sources);
- development of production of organic food products;

- creation of production facilities for the processing of household and industrial waste (according to statistics, 1/7 of the country's territory is littered with garbage, the amount of industrial waste increases annually by hundreds of million tons);
- processing of plastic waste. As in the whole world, in Ukraine the problem of plastic recycling is urgent and private business is included in its solution. So, for example, the "Morshynska" brand updated its packaging design, reducing the amount of plastic used by 15 %.

As already mentioned, the basis of the development of the circular economy is the application of a wide range of innovations and innovations of financial, production, economic, social, ecological direction, without which the implementation of the specified processes is not possible. Considering the essence of the circular economy as a new way of using and consuming resources and material goods, it is appropriate to analyze, in particular, marketing innovations that contribute to the implementation of its main principles. In general, marketing innovations involve the development and implementation of fundamentally new or significantly optimized marketing methods, techniques, technologies and tools in all areas of marketing activity. The main direction of marketing innovations is to meet the growing and constantly changing needs and demands of consumers, optimization of the influence of marketing tools on consumer behavior, expansion of sales markets. With this in mind, marketing innovations of the circular economy allow to achieve the goals presented in **Fig. 6.3**, which produce a synergistic effect for the development of enterprises and industries.

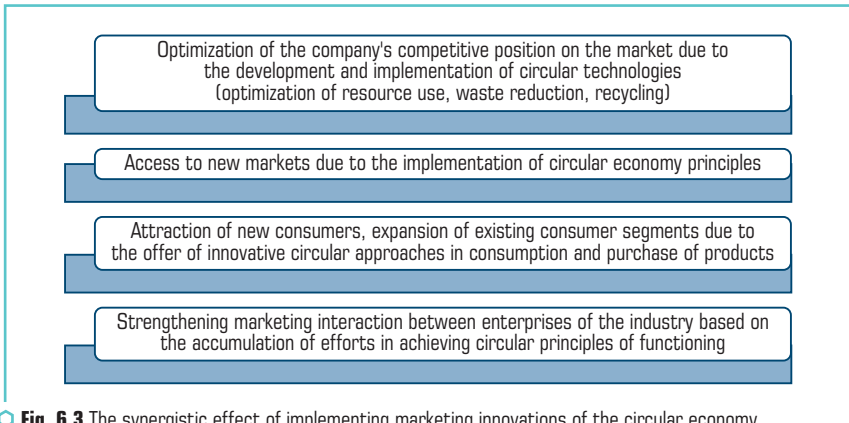


Fig. 6.3 The synergistic effect of implementing marketing innovations of the circular economy
Source: [34]

Marketing innovations of the circular economy are an important component of the implementation of its principles in all spheres of economy, but they are especially important in light industry, in the field of textiles, fashion and design. The textile industry is an important branch of the world economy with an annual turnover of more than 2.5 trillion USD. The fashion segment leads

the textile market. In 2022, it accounted for more than 70 % of global income [9]. However, this industry requires the application of the principles of a circular economy, since greenhouse gas emissions occur throughout the entire life cycle of textile products: from the extraction of raw materials to production, transportation, use and disposal. The impact of textiles on the environment is negative, since textiles often consist of synthetic materials, the impact of which on the environment depends on the type of fiber, its origin and the production process. In addition, many textile products contain carbon, which is released during the incineration of waste. For example, 4–6 % of the EU's "ecological footprint" is caused by textile consumption. From 2025, all European member states will have to create separate collection systems for textile waste [35].

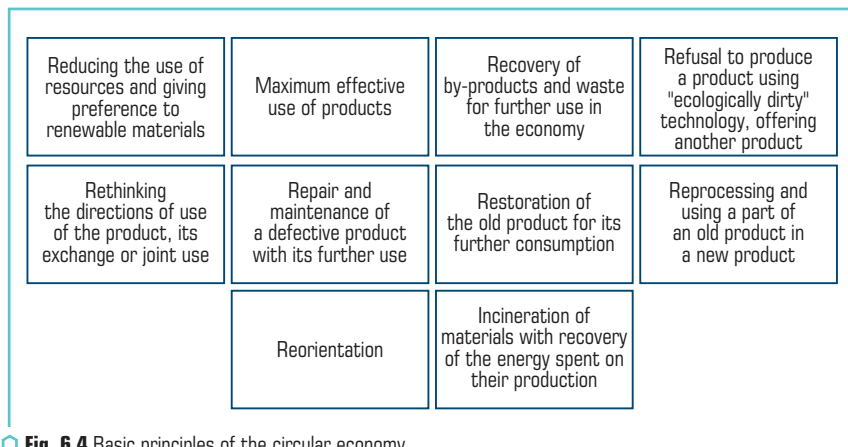
The increase in material extraction in recent years has reduced global circularity from 9.1 % in 2018 to 8.6 % in 2020 and 7.2 % in 2023 [36]. This means that more than 90 % of materials are wasted, lost, or remain unavailable for reuse for years because they are locked in long-term inventory. Among the main business principles that apply to the textile industry, the Global Report on the Circular Gap noted the need to avoid fast fashion for environmentally friendly textiles, to prioritize natural textiles, as well as better quality and longer-lasting clothes, reuse or recycle clothes; the need to buy only what is needed, which means a shift to responsible purchases supported by circular policies such as commodity taxes and service-based business models such as sharing or pay-for-use.

In the implementation of marketing innovations of the circular economy in the field of fashion and design, the main provisions of the National Waste Management Strategy in Ukraine until 2030 are of great importance [37]. In this document, industrial waste is defined as one of the most problematic components of sustainable development, and light industry is included in the list of industries where the main volumes are generated. Among the tasks of the Strategy, the implementation of which will contribute, in particular, to the circular development of business entities in the field of light industry, include the following:

- determination of directions and priorities for the development of secondary resource use;
- wide introduction of public-private partnership, interaction and cooperation;
- provision of financing and implementation of specified measures for further improvement of the management system of waste management on traditional basis [37].

Priority in this regard will be the definition of the main technological processes – the best available technologies for reuse, recycling and disposal of waste and the provision of financial assistance to business entities (loans, grants, etc.) for environmental modernization, introduction of cleaner technologies, creation of own capacities for processing and disposal of waste (**Fig. 6.4**).

We consider it expedient to analyze those of the basic principles of the circular economy "10R" established by the World Economic Forum (**Fig. 6.1, 6.4**) that are effectively implemented by Ukrainian clothing brands and the corresponding marketing innovations that involve their application (**Table 6.1**).



● **Fig. 6.4** Basic principles of the circular economy
 Source: [21, 36]

● **Table 6.1** Marketing innovations of the circular economy in the activities of Ukrainian clothing brands

The principle of circular economy	Marketing innovations	Ukrainian brands
Restoration of the old product for its further consumption	Transformation of vintage clothes found in outlets, resale sites into new products	Hate Date Oversized Studio Tokonikomu Buro26 Better UliUlia Ksenia Schneider
Reprocessing and using a part of an old product in a new product	Creation of bags, backpacks from advertising banners in order to combat marketing production waste	RE:ban
	Creating purses, backpacks and bags from banners, scraps of fabric and unwanted clothes	Potrib
	Production of designer bags and accessories from genuine vintage leather recycled from jackets	Remade
Maximum effective use of products	Refusal of mass production of collections in order not to create a stock and sale and production of exactly the amount of clothes that customers need	The Coat by Katya Silchenko
Recovery of by-products and waste for further use in the economy	Production of clothes from fabric that is in warehouses in remnants	Hate Date
	Using regenerated nylon created from recycled fishing nets	<i>Atelier Handmade</i> IENKI IENKI
Rethinking the directions of use of the product, its exchange or joint use	Transformation from a dress rental service to offering a subscription-based virtual wardrobe	Oh My Look!

Note: compiled by the authors based on materials [38–42]

Therefore, the mentioned marketing innovations are used by Ukrainian clothing brands and contribute to the implementation of the principles of the circular economy. However, it is worth noting that we are talking about small and medium-sized business structures, on the other hand, large enterprises that work in the field of sewing clothes and other textile products are only at the beginning of this path. At the same time, it is worth noting that the products manufactured by some of the mentioned Ukrainian brands are in high demand in foreign markets [40]. The main marketing advantage of light industry products made on the basis of circular economy principles is their uniqueness.

In general, the main principles of the circular economy, which are most often used in this field, are presented in **Fig. 6.5**.

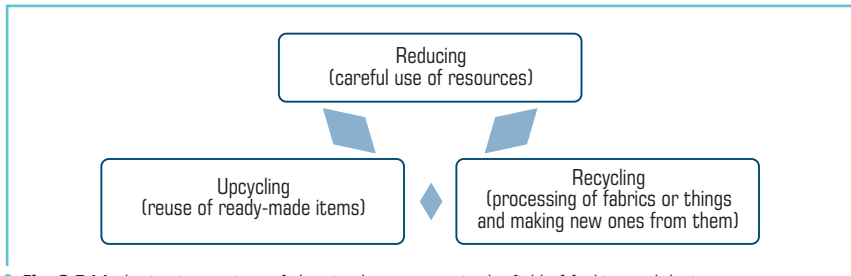


Fig. 6.5 Marketing innovations of the circular economy in the field of fashion and design

In our opinion, it is advisable to use the experience of Great Britain in the application of marketing innovations of the circular economy in the considered area, in particular, paying attention to the following important aspects:

- ensuring a favorable attitude of consumers towards processed products and processing enterprises in general, as well as understanding the importance of processing in the transition to a sustainable society;
- financial and business support for processing enterprises, such as incentives and grants provided by the government and other public bodies;
- creation of "guilds" to provide the technical knowledge, tools and skills needed to expand the recycling business. This should be done with government support and allow access to this kind of knowledge, thus helping businesses of all sizes to do the right thing;
- cooperation between the private and public sectors together with educational institutions can help educate future professionals and especially designers about recycling, circularity and efficient use of resources [43].

In Denmark, circular economy marketing innovations are primarily aimed at sorting textile waste, providing a deeper understanding of consumer behavior and further work on strategies to reduce consumption and switch to products of higher quality and durability, which will become an investment in the future, making repair, exchange and resale more charming; transfer of textile products purchased by households to charitable and private collectors for reuse and recycling,

providing an opportunity to experiment and pilot innovations and technologies for collection, sorting and processing plants, which makes it possible to get closer to closing the textile cycle [35].

It should be noted that these principles are already partially implemented in Ukraine. In this connection, it is worth noting, first of all, the creation of the Podillia Fashion Cluster, among the main goals of which is functioning on the basis of the circular economy, as well as the construction of a processing plant [44].

Secondly, the provision of complex services for the utilization of textile waste, which are provided, in particular, by such companies as "UtilVtorProm", "Ecological Investments" [45, 46] and others. This involves collecting clothes, classifying them into groups, processing, making new fibers. Raw materials produced from textile waste can be used in various industries, including construction, production of interior items, shoe production, and production of new polyester fabrics.

Thirdly, the involvement of consumers in interaction based on the principles of the circular economy. So, for example, the Remade company accepts things for free from people who have decided to get rid of unnecessary leather jackets, they are given a 10 % discount on a permanent basis for a product from their old thing or for buying a ready-made product [39]. The Ukrainian clothing brand Trempel implemented the No Trash project, the purpose of which was to collect and sort any textile that was accepted from anyone for use in three directions: for ecological recycling, for charity, and for sewing new things [47]. Each consumer received a 5 % discount on goods from partner brands.

Among the companies operating in foreign markets, it is worth noting an interesting marketing approach in interaction with consumers, which is used by the Finnish brand ARELA, which launched the concept of sustainable development called "For Good" [48]. This concept includes the aspect that the clothes are designed to avoid waste and to make them more durable and long-lasting in terms of quality and design. The brand educates consumers on how to best care for their clothes to avoid premature disposal. ARELA also offers repair training and repair services, and has a return system to offer the sale of own-brand used items. The company also takes responsibility for its knitwear: it takes back all used knitwear and gives the consumer a 20 % discount on a new product.

Among other foreign brands, it is worth noting Beyond Retro, ASOS Reclaimed Vintage line (production of new products from vintage), Patagonia (creation of shorts and jackets using plastic), Zero Waste Daniel (production entirely from leftovers), Re/Done (production of jeans from old denim products using water-saving methods and the rejection of aggressive chemicals), Anti-form (production of knitwear and other products from used materials), Insecta Shoes (production of shoes from old fabrics and recycled plastic bottles) [49].

In general, the successful implementation of marketing innovations by light industry enterprises will be facilitated by the analysis of product functions in the context of consumer value, that is, the possibility of replacing materials with renewable ones without loss of quality and value for the consumer; optimization of contacts with consumers in order to determine their attitude to the company's use of the principles of the circular economy, influence on the consciousness of consumers using marketing techniques, search for secondary use markets, expansion of presence on them.

CONCLUSIONS

The basis of economic growth at the macro, meso, and micro levels in modern conditions is the process of innovative development, which forms positive qualitative and quantitative changes in any socio-economic system. At the same time, the modern paradigm of global development is the idea of sustainable development. The key tool (mechanism) for the implementation of the Global Sustainable Development Goals is the concept of circular economy as an innovative component of the modern global economy, characterized by breakthrough innovative technologies that, together with innovative business processes, form closed cycles of processing, exchange and consumption.

The circular economy as a new model of economic development, which provides efficient use of limited natural resources and reduces the negative impact on the environment, was born in the early 70s of the last century. As education has shown, the transition to a circular economy is a complex and long process. In general, the evolution of the circular economy can be divided into three stages.

At the first stage (1970–1990), at the beginning of its formation, the circular economy began with the introduction of technologies that reduce environmental pollution. At the same time, work with waste took center stage.

In the second stage (1990–2010), the implementation of environmental payments had a significant impact on the development of the circular economy. During this period, waste-free industrial production technologies were actively developed.

Today, the circular economy has become an integral part of the modern economy at all levels: from the global to the micro level, and the effect of its principles, which are filled with additional content, is expanding and deepening.

The leaders in the development of the circular economy are the leading countries and regions of the world, the EU, the USA, Japan, China, and South Korea. In business, 44 % of the world's 100 largest companies have chosen a circular economy strategy.

From the point of view of the evolutionary development of the circular economy, the most significant results today are demonstrated by the countries of the European Union, where the comprehensive policy of supporting resource efficiency is designed to ensure a complete transition to a circular economy in the foreseeable future, strengthen global competitiveness, and promote sustainable economic growth in the region.

Today, the principles of the circular economy at the micro level are implemented with the help of various new technologies (closed-loop technologies, green technologies, nanotechnologies), various innovative business models, strategies and tools.

In Ukraine, the circular economy is just beginning its formation. Despite the fact that there are already significant first steps on the way to the transition to a circular type of economy, the implementation of the principles of the circular economy faces significant obstacles. The main factors that negatively affect the development of the circular economy in our country are: extremely high prices for transporting raw materials for repeated processing; imperfect logistics infrastructure, mainly poor-quality roads; opacity of the market of secondary raw materials; lack of tariffs

for recycling of secondary resources; low level of environmental tax, which, on the one hand, leaves support for measures aimed at building a circular economy, and on the other hand, does not stimulate manufacturers to implement closed-loop technologies; the practice of public procurement, where the main criterion for choosing a supplier is usually the cheapest offer without taking into account the environmental friendliness and energy efficiency of the purchased products.

Despite the large number of adopted program documents, Ukraine has not yet formed a coherent system of support for the development of the circular economy. Specific rapid changes are needed that will contribute to the formation of a closed cycle economy in our country.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Maistrenko, N. V., Serdiuk, B. M. (20115). Basis the evaluation of efficiency innovation in enterprises. Available at: https://ela.kpi.ua/bitstream/123456789/14310/1/2015_1_Maystrenko.pdf
2. Kosovych, B. (2022). Innovative development of Ukraine in the conditions of war and post-war period. *Economics & Education*, 7 (4), 6–12. doi: <https://doi.org/10.30525/2500-946x/2022-4-1>
3. Kniazevych, A. O. (2018). Upravlinnia infrastrukturnym zabezpechenniam innovatsiinoho rozvytku ekonomiky. Rivne: Volynski oberehy, 362.
4. Horbach, L. M., Kobuk, A. L. (2017). Innovatsiyni rozvytok u suchasnomu sviti: osnovni pidkhody do vyvchennia. Available at: http://www.confcontact.com/2017-ekonomika-i-menedzhment/10_gorbach.htm
5. Boichuk, N. Ya. (2021). Innovatsiyni rozvytok ta potentsial pidpriemstv v Ukraini. *Biznes, Innovatsii, Menedzhment: Problemy ta Perspektyvy*. Available at: <http://confmanagement.kpi.ua/proc/article/view/231791>
6. Hladynets, N. Yu. (2014). National innovation system as a basis for innovative development of industry in Ukraine. Available at: http://dspace-s.msu.edu.ua:8080/bitstream/123456789/39/1/07_Hladynets.pdf
7. Buniak, N. M. (2011). The essence of the national innovation system. *Efektivna ekonomika*, 7. Available at: <http://www.economy.nayka.com.ua/?op=1&z=633>
8. Holod, A. P., Izhevska, O. P., Korkuna, O. I. (2019). Cluster model of the hospitality industry development in a region. *Skhidna yevropa: ekonomika, biznes ta upravlinnia*, 4 (21), 375–380. Available at: http://www.easterneurope-ebm.in.ua/journal/21_2019/60.pdf

9. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions A New European Innovation Agenda. COM/2022/332. 05.07.2022. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52022DC0332>
10. Pro Tsili staloho rozvytku Ukrainy na period do 2030 roku (2019). Ukaz Prezidenta Ukrainy No. 722/2019. 30.09.2019. Available at: <https://zakon.rada.gov.ua/laws/show/722/2019#Text>
11. Yurynets, Z. V. (2016). Formuvannya innovatsiinykh stratehii: teoriia, metodolohiia, praktyka. Lviv: SPOLOM, 412.
12. Yatskevych, I. (2022). Innovation policy of ukraine in the postwar period. *Economy and Society*, 39. doi: <https://doi.org/10.32782/2524-0072/2022-39-53>
13. Silva, F. M. da, Oliveira, E. A. de A. Q., Moraes, M. B. de. (2016). Innovation development process in small and medium technology-based companies. *RAI Revista de Administração Inovação*, 13 (3), 176–189. doi: <https://doi.org/10.1016/j.rai.2016.04.005>
14. Naumov, O., Voronenko, M., Naumova, O., Savina, N., Vyshemyrska, S., Korniychuk, V., Lytvynenko, V.; Babichev, S., Lytvynenko, V. (Eds.) (2022). Using Bayesian Networks to Estimate the Effectiveness of Innovative Projects. *Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2021. Lecture Notes on Data Engineering and Communications Technologies*. Vol. 77. Cham: Springer. doi: https://doi.org/10.1007/978-3-030-82014-5_50
15. Orel, A. (2019). Competitive strategies for innovation and investment development of agricultural production entities. *Ukrainian Journal of Applied Economics*, 4 (4), 411–418. doi: <https://doi.org/10.36887/2415-8453-2019-4-46>
16. Otsinka efektyvnosti innovatsiinoi diialnosti pidpriumstva. Available at: <https://elearn.nubip.edu.ua/mod/book/tool/print/index.php?id=357320>
17. Closing the loop: Commission adopts ambitious new Circular Economy Package to boost competitiveness, create jobs and generate sustainable growth (2015). European Commission – Press release. Available at: http://europa.eu/rapid/press-release_IP-15-6203_en.htm Last accessed: 15.04.2018
18. Baiura, D. (2021). Tsyrukuliarna ekonomika – maibutnie uspishnoi Ukrainy. *Enerho biznes*, 42 (1235).
19. Melnyk, O. H., Zlotnik, M. L. (2020). Analyzing the Status and Tendencies of Circular Economy Development in Lviv Region. *Business Inform*, 2 (505), 125–133. doi: <https://doi.org/10.32983/2222-4459-2020-2-125-133>
20. Model tsyrukuliarnoi ekonomiky (2021). Diia. Biznes. Available at: <https://business.diia.gov.ua/handbook/impact-investment/model-cirkularnoi-ekonomiki>
21. Ruda, M., Yaremchuk, T., Bortnikova, M. (2021). Circular economy is Ukraine: adaptation of European experience. *Management and Entrepreneurship in Ukraine: The Stages of Formation and Problems of Development*, 3 (1), 212–222. doi: <https://doi.org/10.23939/smeu2021.01.212>
22. Towards the circular economy. Vol. 1: an economic and business rationale for an accelerated transition (2013). Ellen McArthur Foundation. Available at: <https://www.ellenmacarthurfoundation.org/towards-the-circular-economy-vol-1-an-economic-and-business-rationale-for-an>

23. Natsionalna dopovid "Tsili Staloho Rozvytku: Ukraina" (2017). Available at: <https://www.kmu.gov.ua/storage/app/sites/1/natsionalna-dopovid-csr-Ukrainy.pdf>
24. Nechytailo, D. (2020). Z chystoho arkusha: yak pratsiuie i chym vyhidna tsyrkuliarna ekonomika. Ekonomichna pravda. Available at: <https://www.epravda.com.ua/columns/2020/09/2/664626/> Last accessed: 17.03.2021
25. Viikman, A., Skonberh, K. (2017). Tsyrukuliarna ekonomika ta perevahy dlia suspilstva. Available at: http://www.clubofrome.org.ua/wp-content/uploads/2017/08/The-Circular-Economy-CoR_UA-2.pdf Last accessed: 17.03.2021
26. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A new Circular Economy Action Plan For a cleaner and more competitive Europe (2020). Document 52020DC0098. COM/2020/98 final. European Commission. Brussels. Available at: <https://bit.ly/3rnvl0s>
27. New EU policy on the "circular" economy: opportunities for Ukraine (2020). Publikatsiia HO "Diksi Hrup", 16.
28. Lykholat, S. M. (2021). Tsyrukuliarna ekonomika yak napriam promyslovoi modernizatsii: perehovyi mizhnarodnyi dosvid. Biznes, innovatsii, menedzhment: problemy ta perspektyvy. Available at: <http://confmanagement.kpi.ua/proc/article/view/230935>
29. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a circular economy: a zero waste programme for Europe" (2014). Brussels. COM(2014) 398 final. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:50edd1fd-01ec-11e4-831f-01aa75e-d71a1.0001.01/DOC_1&format=PDF
30. Kuzior, A., Arefieva, O., Poberezhna, Z., Ihumentsev, O. (2022). The Mechanism of Forming the Strategic Potential of an Enterprise in a Circular Economy. Sustainability, 14 (6), 3258. doi: <https://doi.org/10.3390/su14063258>
31. Varfolomieiev, M., Churikanova, O. (2020). Circular economy as an integral way of ukraine's future in the aspect of globalization. Efektyvna Ekonomika, 5. doi: <https://doi.org/10.32702/2307-2105-2020.5.200>
32. Sergiienko, L. (2016). Directions of reforming of the state policy in provision of a circular economy in the context of international cooperation. Investytsii: praktyka ta dosvid, 23, 100–110. Available at: http://www.investplan.com.ua/pdf/23_2016/24.pdf
33. Stalyi rozvytok kompanii. Shliakhy rozviazannia problem zi smittiam – pershyi krok do tsyrkularnoi ekonomiky (2020). Available at: <https://www.ukrinform.ua/rubric-presshall/2877667-stalij-rozvitok-kompanij-slahi-rozvazanna-problem-zi-smittiam-persij-krok-do-cirkularnoi-ekonomiki.html>
34. Lypych, L. H., Khilukha, O. A., Kushnir, M. A., Volynets, I. H. (2022). Eko-innovatsii v konteksti ekonomiky zamknutoho tsykladu. Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna. Seriia yurydychna, 32, 16–23.

35. Tsykuliarna ekonomika z aktsentom na plastmasy i tekstyl. Dorozhnia karta 2030–2050. Available at: https://www.astar.agency/wp-content/uploads/2023/02/22_3889_ASTAR_CircEco_broshyra_UKR.pdf
36. The circularity gap report 2023. Available at: <https://www.circularity-gap.world/2023>
37. Pro skhvalennia Natsionalnoi stratehii upravlinnia vidkhodamy v Ukraini do 2030 roku (2017). Rozporiadzhennia Kabinetu Ministriv Ukrainy No. 820-r. 08.11.2023. Available at: <https://zakon.rada.gov.ua/laws/show/820-2017-%D1%80#Text>
38. Hate Date, Upcycling Freaks ta ReRe:Sklo: yak ukrainski upcycling-brendy daiut nove zhyttia starym recham. Available at: <https://vctr.media/ua/hate-date-upcycling-freaks-ta-teresklo-yak-ukrayinski-upcycling-brendi-dayut-nove-zhyttia-starim-recham-185730/>
39. Rodygina, A. (2020). 20 vidomikh ukrainskikh sustainable-brendiv. Available at: <https://elle.ua/moda/fashion-blog/20-vidomih-ukrainskih-sustainable-brendiv/>
40. Modno, stylno, ekolohichno: yak odiahatysia, shchob ne shkodyty pryrodi ta yaki ye v Ukraini ekobrendy (2021). Available at: <https://tsn.ua/exclusive/modno-stilno-ekologichno-yak-ody-agatisya-schob-ne-shkoditi-prirodi-ta-yaki-ye-v-ukrayini-ekobrendi-1766455.html>
41. 4 ukrainski brendy, yaki pratsiuut z pereroblenym plastykom (2021). Available at: <https://vogue.ua/article/fashion/brend/4-ukrainskih-brenda-kotorye-rabotayut-s-pererobotanym-plastykom-44840.html>
42. Stepanenko, V. (2022). Dlia prodazhu chy na utylizatsiiu? Available at: <https://media.zagoriy.foundation/velyka-istoriya/dlya-prodazhu-chy-na-utylizacziyu-kudy-viddaty-nepotribnyj-odyag/>
43. Challenges and opportunities for scaling up upcycling businesses – The case of textile and wood upcycling businesses in the UK (2021). Available at: <https://knowledge-hub.circle-lab.com/article/8942?n=Challenges-and-opportunities-for-scaling-up-upcycling-businesses-%E2%80%93-The-case-of-textile-and-wood-upcycling-businesses>
44. Podillia Fashion Cluster: narodzhenyi viinoiu (2022). Available at: <https://www.clusters.org.ua/success-stories/podillia-fashion-cluster-narodzhennij-vijnoyu/>
45. Posluhy. Ekolohichni Investytsii. Available at: <https://ecological.investments/poslugi/>
46. Utylizatsiia odiahu. Available at: <https://xn--80ancaco1ch7azg.xn--j1amh/uk/utilizatsiya-othodov/utilizatsiya-odezhdy/>
47. Ukrainskyi brend pochav pryimaty nepotribnyi odiah na pererobku (2020). Available at: https://lb.ua/society/2020/02/05/449093_ukrainskiy_brend_nachal_prinimat.html
48. For Good. Available at: <https://www.arelastudio.com/pages/for-good>
49. Opys brendiv odiahu, yaki vypuskaiut odiah za dopomohoiu metodu pererobky. Available at: <https://newsdaily.org.ua/522-9-brendiv-odyagu-yaki-vipuskayut-odyag-za-dopomogoyu-metodu-pererobki.html>

ECONOMIC AND CYBER SECURITY

Victor Krasnobayev, Alina Yanko, Alina Hlushko, Oleg Kruk, Oleksandr Kruk, Vitalii Gakh,
Svitlana Onyshchenko, Oleksandra Maslii, Oleksandr Kivshyk, Kateryna Potapova,
Mykola Nalyvaichuk, Vasyl Meliukh, Stanislav Gurynenko, Kostiantyn Koliada,
Alexandre Scherbyna, Anastasiia Poltorak, Svitlana Tyshchenko, Olha Khrystenko,
Volodimir Ribachuk, Vitalii Kuzoma, Viktoriia Stamat, Maksym Kolesnyk, Olena Arefieva,
Dmytro Onoprienko, Yuliia Kovalenko, Tetiana Ostapenko, Iryna Hrashchenko

Collective monograph

Technical editor I. Prudius
Desktop publishing T. Serhienko
Cover photo Copyright © 2023 Canva

PC TECHNOLOGY CENTER
Published in November 2023
Enlisting the subject of publishing No. 4452 – 10.12.2012
Address: Shatylova dacha str., 4, Kharkiv, Ukraine, 61165
