Edited by
Serhii Yevseiev, Ruslan Hryshchuk,
Kateryna Molodetska, Mariia Nazarkevych

MODELING OF SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURE FACILITIES

Monograph

2022

UDC 004.056
M78

Reviewers:
Dudykevych Valerii, Doctor of Technical Science, Professor, Head of the Department of Information Security of Lviv Polytechnic National University;
Korchenko Alexandr, Doctor of Technical Sciences, Professor, Head of the Department of Information Technology Security of National Aviation University.

M78 **Authors:**
Edited by **Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych**
Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych, Volodymyr Hrytsyk, Oleksandr Milov, Olha Korol, Stanislav Milevskyi, Roman Korolev, Serhii Pohasii, Andrii Tkachov, Yevgen Melenti, Oleksandr Lavrut, Alla Havrylova, Serhii Herasymov, Halyna Holotaistrova, Dmytro Avramenko, Roman Vozniak, Oleksandr Voitko, Kseniia Yerhidzei, Serhii Mykus, Yurii Pribyliev, Olena Akhiiezer, Mykhailo Shyshkin, Ivan Opirskyy, Oleh Harasymchuk, Olha Mykhaylova, Yuriy Nakonechnyy, Marta Stakhiv, Bogdan Tomashevsky
Development of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

The monograph discusses the methodology for cooperative conflict interaction modeling of security system agents. The concept of modeling the structure and functioning of the security system of critical infrastructure facilities is demonstrated. The method for assessing forecast of social impact in regional communities is presented. Counteracting the strategic manipulation of public opinion in decision-making by actors of social networking services based on the conceptual model for managed self-organization in social networking services are developed. Algorithms for thinning the critical infrastructure identification system and their software are implemented.
The monograph is intended for teachers, researchers and engineering staff in the field of cybersecurity, information technology, social engineering, communication systems, computer technology, automated control systems and economic information security, as well as for adjuncts, graduate students and senior students of relevant specialties.
Figures 99, Tables 24, References 176 items.

9 786177 319572

AUTHORS

SERHII YEVSEIEV
Doctor of Technical Science, Professor, Head of Department
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0003-1647-6444

RUSLAN HRYSHCHUK
Doctor of Technical Science, Professor, Honored Worker
of Science and Technology of Ukraine, Head of Faculty
Faculty of State Secrets Protection and Information Warfare
Sergei Korolyov Zhytomyr Military Institute
ORCID ID: https://orcid.org/0000-0001-9985-8477

KATERYNA MOLODETSKA
Doctor of Technical Science, Professor
Department of Computer Technology and Systems Modelling
Polissia National University
ORCID ID: https://orcid.org/0000-0001-9864-2463

MARIIA NAZARKEVYCH
Doctor of Technical Science, Professor
Department of Information Systems and Networks
Institute of Computer Sciences and Information Technologies
Lviv Polytechnic National University
ORCID ID: https://orcid.org/0000-0002-6528-9867

VOLODYMYR HRYTSYK
Doctor of Technical Science, Professor
Department of Automated Control Systems
Lviv Polytechnic National University
ORCID ID: https://orcid.org/0000-0002-9696-5805

OLEKSANDR MILOV
Doctor of Technical Science, Professor
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0001-6135-2120

OLHA KOROL
PhD, Associate Professor
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0002-8733-9984

STANISLAV MILEVSKYI
PhD, Associate Professor
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0001-5087-7036

ROMAN KOROLEV
PhD, Associate Professor
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: http://orcid.org/0000-0002-7948-5914

SERHII POHASII
PhD, Associate Professor
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0002-4540-3693

ANDRII TKACHOV
PhD, Associate Professor
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0003-1428-0173

YEVGEN MELENTI
PhD, Associate Professor
Special Department No. 3 «Tactical-special training,
marksmanship training and special physical training»
Juridical Personnel Training Institute for Security Service
of Ukraine
Yaroslav Mudryi National Law University
ORCID ID: https://orcid.org/0000-0003-2955-2469

OLEKSANDR LAVRUT
Doctor of Engineering Sciences, Professor
Department of Tactics
Hetman Petro Sahaidachnyi National Army Academy
ORCID ID: https://orcid.org/0000-0002-4909-6723

ALLA HAVRYLOVA
Senior Lecturer
Department of Cyber Security
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0002-2015-8927

SERHII HERASYMOV
Doctor of Technical Science, Professor, Head of Department
Department of Weapons and Military Equipment Operation
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0003-1810-0387

HALYNA HOLOTAISTROVA
Associate Professor
Department of Computer Mathematics and Data Analysis
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0001-8349-6571

DMYTRO AVRAMENKO
Senior Researcher
Research Department
Institute of Troops (Forces) Support and Information
Technologies
National Defence University of Ukraine named after Ivan
Chernyakhovskyi
ORCID ID: https://orcid.org/0000-0003-1892-380X

ROMAN VOZNIAK
PhD, Head of Laboratory
Head of the Research Laboratory of Information Technology
Problems Research Department
Institute of Troops (Forces) Support and Information
Technologies
National Defence University of Ukraine named after Ivan
Chernyakhovskyi
ORCID ID: https://orcid.org/0000-0002-3789-2837

OLEKSANDR VOITKO
PhD, Deputy Head of Department
Department of Information Technologies and Information
Security Employment
Institute of the Troops (Forces) Support and Information
Technologies
National Defence University of Ukraine named after Ivan
Chernyakhovskyi
ORCID ID: https://orcid.org/0000-0002-4610-4476

KSENIIA YERHIDZEI
PhD, Head of Laboratory
Research Laboratory
Institute of Troops (Forces) and Information Technologies
National Defence University of Ukraine named after Ivan
Chernyakhovskyi
ORCID ID: https://orcid.org/0000-0003-4634-133X

SERHII MYKUS
Doctor of Technical Sciences, Professor, Head of Department
Department of Information Technology Application and
Information Security
Institute of Troops (Forces) Support and Information
Technologies
National Defence University of Ukraine named after Ivan
Chernyakhovskyi
ORCID ID: https://orcid.org/0000-0002-7103-4166

YURII PRIBYLIEV
Doctor of Technical Science, Professor
Department of Information Technologies Employment and
Information Security
National Defence University of Ukraine named after Ivan
Chernyakhovskyi
ORCID ID: https://orcid.org/0000-0003-1941-3561

OLENA AKHIIEZER
PhD, Associate Professor, Head of Department
Department of Computer Mathematics and Data Analysis
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: http://orcid.org/0000-0002-7087-9749

MYKHAILO SHYSHKIN
PhD, Associate Professor
Department of Industrial and Biomedical Electronics
National Technical University «Kharkiv Polytechnic Institute»
ORCID ID: https://orcid.org/0000-0002-2276-7259

IVAN OPIRSKYY
Doctor of Technical Sciences, Professor
Department of Information Protection
Lviv Polytechnic National University
ORCID ID: https://orcid.org/0000-0002-8461-8996

OLEH HARASYMCHUK
PhD, Associate Professor
Department of Information Protection
Lviv Polytechnic National University
ORCID ID: https://orcid.org/0000-0002-8742-8872

OLHA MYKHAYLOVA
PhD, Associate Professor
Department of Information Protection
Lviv Polytechnic National University
ORCID ID: https://orcid.org/0000-0002-3086-3160

YURIY NAKONECHNYY
PhD, Associate Professor
Department of Information Protection
Lviv Polytechnic National University
ORCID ID: https://orcid.org/0000-0002-6046-6190

MARTA STAKHIV
PhD, Associate Professor
Department of Information Protection
Lviv Polytechnic National University
ORCID ID: https://orcid.org/0000-0002-4094-2081

BOGDAN TOMASHEVSKY
PhD, Associate Professor
Department of Cyber Security
Ternopil Ivan Puluj National Technical University
ORCID ID: https://orcid.org/0000-0002-1934-4773

ABSTRACT

The development of Industry 4.0 technologies is based on the rapid growth of the computing capabilities of mobile wireless technologies, which has made it possible to significantly expand the range of digital services and form a conglomeration of socio-cyber-physical systems and smart technologies. The First Section discusses the issues of building security systems based on the proposed Concept of multi-contour security systems, taking into account the hybridity and synergy of modern targeted cyber-attacks, their integration with social engineering methods. This approach not only increases the level of security, but also forms an objective approach to the use of post-quantum security mechanisms based on the proposed Lotka-Volterra models.

The Second Section analyzes the features of the functioning of social Internet services and establishes their role in ensuring the information security of the state. An approach is proposed to identify signs of threats in the text content of social Internet services, which will allow to quickly respond to changing situations and effectively counteract such threats. A classifier of information security profiles of users of social Internet services has been developed to assess the level of their danger as potential participants in disinformation campaigns. A method for identifying and evaluating the information and psychological impact on user communities in services is proposed. Models of conflict interaction of user groups in social Internet services are considered on the example of civil movements. To effectively counter threats to information security of the state, it is proposed to use the concept of synergistic user interaction and self-organization processes in a virtual community. Particular attention is paid to countering the manipulation of public opinion in the decision-making process by users of social Internet services.

The Third Section proposes a biometric security system that works to authenticate users based on a comparison of their fingerprints and certain templates stored in a biometric database. A method for determining the contour based on the passage of a curve and the filtering function of contour lines has been developed. The stage of skeletal identification is analyzed in detail. The Ateb-Gabor method with wave thinning has been developed. The performance of skeletal algorithms such as the Zhang-Suen thinning algorithm, the Hilditch algorithm, and the Ateb-Gabor method with wave decimation is analyzed. The presented results of experiments with biometric fingerprints based on the NIST Special Database 302 database showed the effectiveness of the proposed method. The software and firmware were developed using the Arduino Nano.

KEYWORDS

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

A	availability
ABS	automated banking system
Aff	affiliation
AFIS	automatic fingerprint identification
Au	authenticity
C	confidentiality
CCC McEliece	crypto code constructs McEliece/Niederreiter
CI	critical infrastructure
CIFS	critical infrastructure facilities systems
CIO	critical infrastructure objects
CPS	cyber-physical systems
CPSS	cyberphysical social system
CS	cybersecurity
DCS	distributed control systems
DDoS	denial of service attack
GIS	geospatial information systems
I	integrity
ICS	information and communication networks
IoTS	internet of things systems
IR	information resources
IS	information security
ISS	information security system
LDPC	low-density parity-check codes
LSI	a latent semantic indexing method
MCC	Matthew correlation coefficient
MCMC	method of Markov chain Monte Carlo
PLC	programmable logic controllers
SCADA	supervisory control and data acquisition
SI	information security

CIRCLE OF READERS AND SCOPE OF APPLICATION

Methodology for Cooperative Conflict Interaction Modeling of Security System Agents is proposed. The concept of modeling the structure and functioning of the security system of critical infrastructure facilities is demonstrated for development of a model for the implementation of a terrorist act and the degree of security of the cyber system of a critical infrastructure object. Lotka-Volterra model are used for assessing the level of security of critical infrastructure facilities. The method for assessing forecast of social impact in regional communities as a case of socio-cyber-physical systems security concept is presented.

Methodological aspects of providing information security of an individual, society and state in social networking services are investigated. Identification of threats to the information security of the state in the text content of social networking services is used for information security profiles of actors in social networking services, their classification, and information-psychological influence on actors and approaches to its evaluation. The model of conflictual interaction of civic movements in social networking services.

Counteracting the strategic manipulation of public opinion in decision-making by actors of social networking services based on the conceptual model for managed self-organization in social networking services are developed.

The problems of physical access to critical infrastructure based on analysis of biometric protection systems as a class of authentication systems are introduces. Algorithms for thinning the critical infrastructure identification system and their software are implemented.

For teachers, scientific and engineering staff in the field of cybersecurity, information technology, social engineering, communication systems, computer technology, automated control systems and economic information security, as well as for adjuncts, graduate students and senior students of relevant specialties.

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.

1 INTRODUCTION

The development of industry 4.0 technologies makes it possible to create fundamentally new technologies and systems based on the rapid development of computing resources. The formation of socio-cyber-physical systems is based on the integration of digital mobile, wireless technologies with classical Internet technologies, social networks and Internet of Things. This approach allows the formation of smart cities based on the hybridity of smart technologies with mesh networks, which allows the integration of technologies among themselves and the erasing of the boundaries of their use, on the one hand. On the other hand, it forms a vector of cyber threats and targeted attacks based on the hybridity and synergy of modern threats.

The logical and physical structure of socio-cyber-physical systems are discussed in Section 1. In our opinion, it belongs to critical infrastructure objects. Security systems for critical infrastructure objects are proposed based on the Lotka-Volterra model, which take into account signs of synergy and hybridity of targeted attacks, as well as the computational and financial capabilities of cyber-intruders. The concept of security of socio-cyber-physical systems is proposed, which takes into account the integration of technologies, security systems of individual components of a smart city and the complexing of cyber threats into security components. This approach provides an objective assessment of the current state of infrastructure security both for critical infrastructure objects and socio-cyber-physical systems, to form security mechanisms based on post-quantum algorithms — McEliece and Niederreiter crypto-code constructions on various codes, taking into account the degree of secrecy of information flows.

The features of the social Internet services functioning and establishes their role in ensuring the information security of the state are analyzed in the Second Section. Based on the identification of signs of threats in the text content of social Internet services, a classifier of information security profiles of users of social Internet services is proposed to assess the level of their danger as potential participants in disinformation campaigns. Models of conflict interaction of user groups in social Internet services are proposed on the example of civil movements, which allows timely formation of preventive measures against threats to the information security of the state. Particular attention is paid to countering the manipulation of public opinion in the decision-making process by users of social Internet services.

In the Third Section, based on the analysis of new hardware technologies of mobile sensors and the importance of data protection, a biometric security system is proposed that provides an authenticity service. A method is proposed for providing an authenticity service by contour detection based on passing a curve and a contour line filtering function. To implement the skeletonization process, the transformation of a set of pixels of an image object into a corresponding graph is used, which makes it possible to form a vector image. Fingerprint comparison is performed by searching for key points on images, searching for corresponding reference points on images,

determining the values of attributes of key points on images. As a result, the decision is made that the images are identical if these images have a common set of identical corresponding singular points. To provide confidentiality and integrity services in socio-cyber-physical systems, it is proposed to use post-quantum McEliece algorithms based on crypto-code structures on algebro-geometric, defective and LDPC codes.

The material of the monograph is scientifically new and, in many respects, contains its own results of scientific research obtained by the authors and published in a number of scientific articles. The matter is presented at a high scientific and, at the same time, accessible level, and is properly structured.

2 METHODOLOGY FOR COOPERATIVE CONFLICT INTERACTION MODELING OF SECURITY SYSTEM AGENTS

ABSTRACT

This Section is deal with the methodology for Cooperative Conflict Interaction Modeling of Security System Agents.

The Concept of their integration with social engineering methods, taking into account the hybridity and synergy of modern targeted cyber-attacks, is proposed. The proposed Concept provides the basis for the formation of security systems in the post-quantum period and provides a fundamentally new approach to the objectivity of assessing cyber threats. In addition, not only the signs of threats such as synergy and hybridity are taken into account, but also the integration and globalization of technologies, as well as the form of ownership, which can technically and materially affect the final elements of the socio-cyber-physical systems infrastructure.

As a case the model for the implementation of a terrorist act and the degree of security of the cyber system of a critical infrastructure object was developed.

This approach not only increases the level of security, but also forms an objective approach to use of post-quantum security mechanisms based on the proposed Lotka-Volterra models. A method for assessing the security of cyber-physical systems based on the Lotka-Volterra model was developed. As a demonstration of method the security model for cyber-physical systems based on the «predator-prey» model, taking into account the relationship between «prey species» and «predator species» was realized. Also development of a method for assessing the security of cyber-physical systems. The set of proposed models allows to design the method of assessing the level of security of critical infrastructure facilities was developed. The practical implementation of this method was used as a method for assessing forecast of social impact in regional communities.

KEYWORDS

Multi-loop security systems, targeted cyber-attacks, post-quantum security mechanisms, Lotka-Volterra model, cyber-physical systems, critical infrastructure, social impact, regional communities.

The development of the social aspect of the world community is closely related to the expansion of the range of digital services in cyberspace, in which social networks occupy a special place. The leading states of the world conduct information operations in this environment to achieve geopolitical goals. Such processes are reflected in real social and political life. This allows to influence not only the social groups of society, but also to ensure manipulation in political «games», in the conduct of hybrid wars. The section proposes a threat model that takes into account possible synergistic/emergent features of complexing modern targeted threats and their hybridity. The concept

of assessing the level of protection of critical infrastructure objects (CIO) has been developed, which allows creating a unified database of threats, assessing the signs of their synergy and hybridity, identifying critical points in the CIO infrastructure, determining the level of compliance with regulators' requirements, and the state of the protection system. The mathematical apparatus and many models underlying the concept can be used for all CIOs, which make it possible to unify preventive measures and increase the level of safety.

Security models of cyber-physical systems based on the Lotka-Volterra «predator-prey» model are proposed, namely, taking into account the computational capabilities and the direction of targeted cyberattacks, the possible competition of attackers in relation to the «prey», and also the relationship between «types of prey» and «types of predator». The proposed method for evaluating the security of cyber-physical systems is based on the developed threat classifier, allows to assess the current level of security and dynamically generate recommendations regarding the distribution of limited protection resources based on an expert assessment of known threats. This approach makes it possible to carry out dynamic modeling in offline mode, which allows, based on threat analysis, to timely determine the capabilities of intruders and form preventive protection measures.

The formation of socio-cyber-physical systems is based on the integration of digital mobile, wireless technologies with classical Internet technologies, social networks and Internet things. This approach allows the formation of smart cities based on the hybridity of smart technologies with mesh networks, which allows the integration of technologies among themselves and the erasing of the boundaries of their use, on the one hand. On the other hand, it forms a vector of cyber threats and targeted attacks based on the hybridity and synergy of modern threats. The concept of security of socio-cyber-physical systems is proposed, which takes into account the integration of technologies, security systems of individual components of a smart city and the integration of cyber threats into security components.

To ensure security in such systems, it is proposed to use post-quantum cryptography algorithms on crypto-code structures to provide security services. The proposed mechanisms provide a level of stability (2^{30}–2^{35} group operations), the crypto-transformation speed is comparable to the speed of block-symmetric encryption and reliability (P_{err} 10^{-9}–10^{-12}), while taking into account the level of secrecy of the information itself, which makes it possible to effectively use various coding mechanisms.

2.1 THE CONCEPT OF MODELING THE STRUCTURE AND FUNCTIONING OF THE SECURITY SYSTEM OF CRITICAL INFRASTRUCTURE FACILITIES

Critical infrastructure (CI) supports the basic services necessary for the functioning of a complex modern society. Serious disruptions in the provision of services such as transport and energy can leave large populations vulnerable to shortages of food, electricity and fuel, and other basic necessities. Dependence on timely automated supply chains can also exacerbate the impact.

Major natural disasters are good examples of how the destruction or degradation of such services affects populations. Large-scale disruption to these services can be triggered by cyberattacks aimed at undermining confidence in the state and designed to deplete emergency services, medical and police services. CIs provide the foundation for the national economy, security, and health care. In [1], on the basis of intelligence data, the main results in the field of cyber terrorism focused on critical infrastructure facilities are presented (**Table 2.1**). However, the limitation of this work is only a description of the current state of cyber terrorism in the absence of recommendations on adequate countermeasures and measures to create a security system for critical infrastructure facilities.

● **Table 2.1** Aspects of Critical Infrastructure Cyberterrorism

Key results	Emerging Trends Indicate Terrorists Expanding Cyberattack Opportunities
	The potential for economic damage, the individually initiated and anonymous nature of cyberattacks are well aligned with the ideological beliefs, strategic goals and tactics of many terrorists
	The growing reliance of businesses and other businesses on cyber technology, including interconnected networks and remote access, creates new and growing vulnerabilities that will be exploited by tech-savvy terrorists
	The proliferation of cyber technology and expertise, and the general availability of online hacking tools and «hackers for hire» offer terrorists incentives to adopt cyberattack strategies
Future strategies	Cyberattacks will become more attractive as companies' dependence on cyber technology grows, terrorists improve their cyberattack capabilities by keeping up with new technologies and overcoming countermeasures
	The availability of cyber technology and expertise such as online hacking tools and hired hackers provide resources to empower their own cyberattack capabilities
	The emerging trend to post hacker-related content on their websites indicates their intention to develop more robust cyber strategies in the near future
Possible targets	Potential targets are likely to expand to include a wider range of organizations. and critical infrastructure that terrorists associate with symbols of power
	The international nature of cyberattacks means that many more attackers will be able to attack more remote targets (global communication makes the distance between the cyberattacker and the target irrelevant)
Possible indicators	An increase in the number of statements calling for the use of cyberattack methods
	An increase in the number of messages published on sites about the committed cyberattacks
	Suspicious cyberattacks or increased frequency, creativity, or seriousness versus traditional targets
	Evidence that terrorists are recruiting or seeking services from persons with cyber capabilities

It can be assumed that systems for managing critical infrastructure facilities are the most attractive targets for cyberattacks. Therefore, many works are devoted to the description of the structure, operation and safety of control systems, such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other configurations of control systems, such as programmable logic controllers (PLC) [2–6].

Based on the analysis [1, 7–14], the following definitions were introduced:

— Critical Infrastructure Facilities Systems (CIFS) – a set of automated control systems (dispatching) that ensure the interaction of information and communication networks (ICS) CIF, destruction/failure to operate significantly affects the level of information and/or cybersecurity of the state.

— CIF information resources (IR) – information resources circulating in ICS CIF, modification and/or destruction of which can lead to partial or complete destruction of CIF.

— Confidentiality – protection of CIF IR from passive attacks.

— Confidentiality of the CIF system – a property of the information security system (ISS) of the CIF, which ensures security during transmission.

— Integrity – protection of the CIF IR during storage and/or modification of the IR CIF only by an authorized user (process).

— The integrity of the CIF system – a property of the CIF ISS, which ensures safety during storage, and/or modification of the CIF IR only by an authorized user (process).

— Availability – an access to the CIF IR of an authorized user.

— The accessibility of the CIF system – a property of the information security system that provides access to the IR without restrictions in accordance with the established security model.

— Authenticity – confirmation of the authenticity of the IR CIF. The authenticity of the CIF system is a property of the information security system, which ensures the authenticity of the information source.

— The continuity of the business processes of the CIF system is a property of the information security system, which ensures the formation of a security loop for the business processes of the CIF, which makes it possible to resist blocking the main functions or the destruction of the CIF.

— Security of CIF IR – the state of security of the CIF, which provides security services.

— Threats of CIF RI – a set of technogenic and anthropogenic threats, the integration of which can lead to a synergistic effect, which significantly increases the risks of the implementation of threats to the elements of the CIF.

Threats to information are expressed in violation of its availability, integrity, authenticity and confidentiality.

Fig. 2.1 shows a structural diagram of a synergistic threat model for the elements of the infrastructure of the CIF.

The presented threat model, using the principles of universality, makes it possible to take into account not only possible synergetic/emergent features of the integration of modern target threats into security components, but also their hybridity. This approach makes it possible to form a single (unified) base for classifying threats on the CIF, taking into account their categorization, goals and possible damage, which greatly simplifies the understanding of potential terrorist attacks on the elements of the CIF infrastructure.

For the formation of a general classifier of threats to the elements of the infrastructure of the OCI it is proposed in **Fig. 2.2, 2.3**, the procedure for forming a classifier is divided into

two stages. At the first stage, based on the experts' assessment of the threats and their impact on the security services of the information security information system, a single base of threat vectors is formed, which can be implemented by attackers at various control systems.

At the second stage, on the basis of the proposed expressions, the probabilities of the implementation of threats, the possibility of their synergistic and/or hybrid impact on infrastructure elements are calculated. In this case, the synergistic effect is understood as the impact of threats on one of the security components: cybersecurity (CS), information security (IS) or information security (SI). This approach makes it possible to significantly simplify the classification of threats and/or terrorist acts, to form dependencies between threats and security services, to define hybrid threats, by which it is proposed to understand the aggregation of the impact on one of the security services in all security components. The classifier consists of 6 platforms.

The first platform defines the level of criticality of the implementation of a threat (terrorist attack) as critical, high, medium, low, very low. The second platform is a composite of security: CS, IS, SI. The third platform determines the focus of the threat on one of the security services, which allows assessing the possibility of a synergistic effect of threats on elements of critical infrastructure.
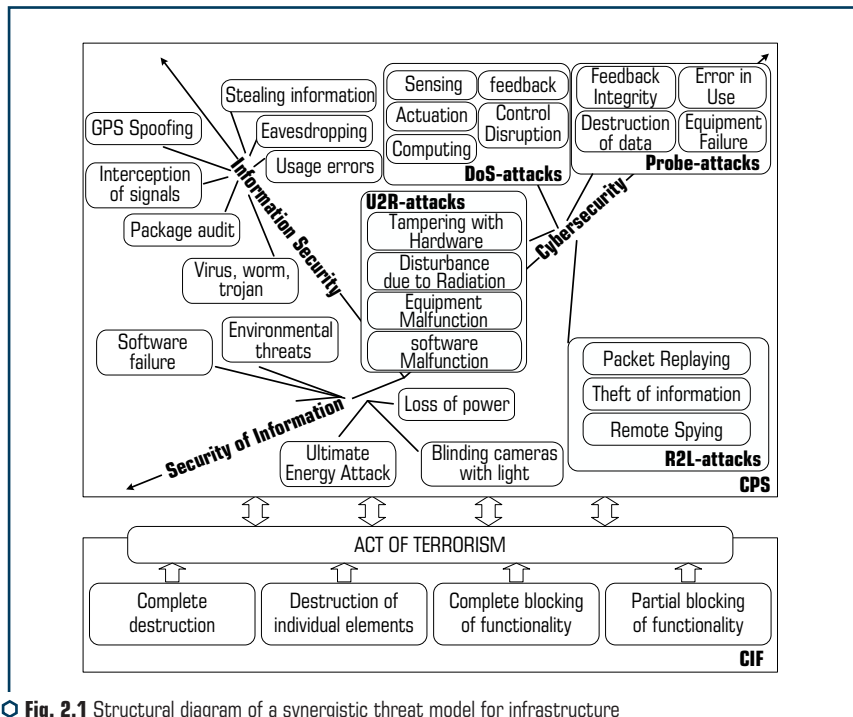
○ **Fig. 2.1** Structural diagram of a synergistic threat model for infrastructure elements of critical infrastructure facilities
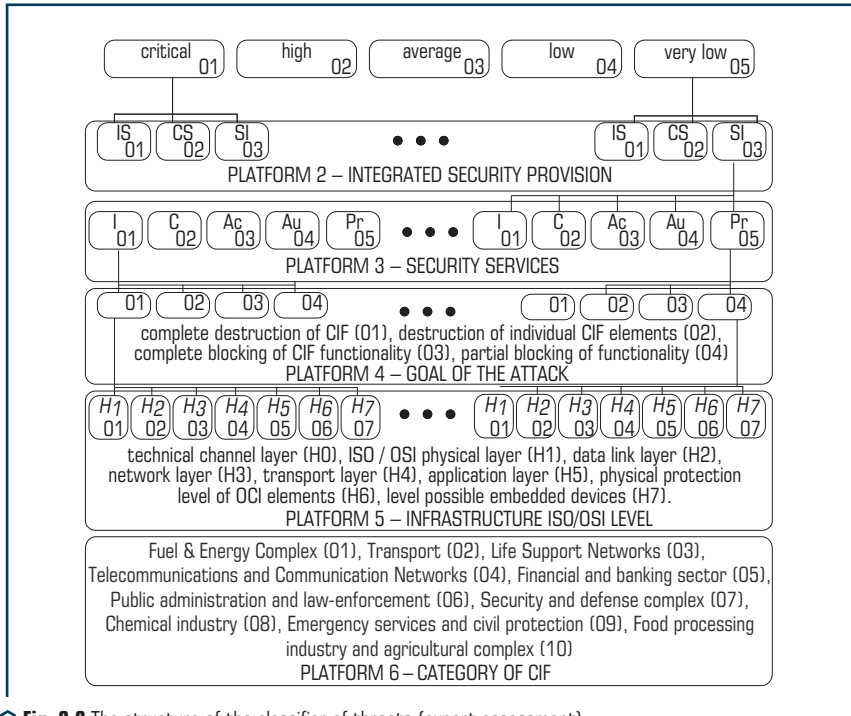
○ **Fig. 2.2** The structure of the classifier of threats (expert assessment)

The fourth platform defines the purpose of the terrorist attack – complete destruction of CIF (01), destruction of individual CIF elements (02), complete blocking of CIF functionality (03), partial blocking of functionality (04).

The fifth platform allows to determine the level of impact of the threat (terrorist attack) on the elements of the CIF infrastructure. Offered: technical channel layer (H_0), ISO/OSI physical layer (H_1), data link layer (H_2), network layer (H_3), transport layer (H_4), application layer (H_5), physical protection level of CPS CIF elements (H_6), level of possible embedded devices (H_7).

The sixth platform defines membership in the CIF category. For further research, it is proposed, in accordance with [15], to consider the following categories:

– fuel and energy complex (01);

– transport (02);

– life support networks (03);

– telecommunications and communication networks (04);

– banking and financial sector (05);

– public administration and law enforcement agencies (06);

– security and defense complex (07);
– chemical industry (08);
– emergency services and civil protection (09);
– food industry and agro-industrial complex (10).

STEP 1. FORMATION OF METRIC FACTORS OF THREATS

$$w_j^{CPS\ CIF} = \frac{1}{K} \sum_{i=1}^{N} \sum_{k=1}^{K} w_j^{CPS\ CIF}{}_{ik}$$

STEP 2. FORMATION OF WEIGHT COEFFICIENTS OF THE MANIFESTATION OF THREATS

$$\alpha_i^{CPS\ CIF}, i \in \left[0.067; 0.133; 0.2; 0.267; 0.333 \right]$$

STEP 3. DETERMINING THE IMPLEMENTATION OF EACH THREAT

$$w_j^{CPS\ CIF}{}_i P_j^{CPS\ CIF}{}_i = \frac{1}{K} P_j^{CPS\ CIF}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIF}{}_{ik}, \text{ where } P_j^{CPS\ CIF}{}_i \in \left\{ \alpha_i^{CPS\ CIF} \right\}$$

STEP 4. DETERMINING THE IMPLEMENTATION OF THREATS ON THE SECURITY SERVICE

$$W_{synerg}^{CFS\ CIF\ C} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ C} \alpha_i^{CPS\ CIF\ C} \cdots W_{synerg}^{CFS\ CIF\ Aff} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Aff} \alpha_i^{CPS\ CIF\ Aff}$$

STEP 5. DETERMINATION OF TOTAL THREATS TO THE COMPOSITION OF SECURITY

$$W_{synerg}^{IS} = \sum_{i=1}^{N} \left(\sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ C} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ I} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ A} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Au} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Aff} \right) \alpha_i^{CPS\ CIF}$$

STEP 6. DETERMINING THE ECONOMIC COSTS OF ATTACK PREVENTION

$$Tr_R^{CPS\ CIF\ A} = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \forall Tr_i \in Tr \Rightarrow Tr_L^{CPS\ CIF} = \arg \max_{\forall Tr_i \in Tr_C^D} K_i^D \cdot K_i^A$$

determined automatically based on mathematical expressions

○ **Fig. 2.3** The structure of the threat classifier (automatic calculations)

To verify the assessment of experts, let's use the approach proposed in [1, 2, 9]. When conducting an expert assessment for the objectivity of the judgments of experts, let's use the weight coefficients of the competence of experts (k_k) presented in **Table 2.2**.

The total assessment of the i-th threat is determined by the number of experts according to the expression:

$$\tilde{x}_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K},$$

(2.1)

where x_k is assessment of the k-th expert in the flow of the i-th threat; k_k is the level of the expert's competence; K is the number of experts.

● **Table 2.2** Expertise weighting factor

No. of salary	Qualification of experts	Weight coefficient value (k_k)
1	International expert in the field of IS, CS, SI	1.0
2	National expert in the field of IS, CS, SI	0.95
3	Certified international specialist in the field of IS, CS, SI	0.9
4	Full Doctor of Science in IS, CS, SI	0.9
5	Director of security	0.85
6	Doctor of Philosophy in IS, CS, SI	0.8
7	Security officer	0.7
8	System Administrator	0.6
9	Security Engineer	0.5
10	Postgraduate student in the field of IS, CS, SI	0.4

A measure of the consistency of expert assessments is the variance, which is determined by the expression:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - \tilde{x}_i\right)^2.$$

(2.2)

The statistical probability of the obtained results $1 - \alpha_i$ will be: $[\tilde{x}_i - \Delta, \tilde{x}_i + \Delta]$, where the quantity x_i is distributed according to the normal law centered at $\tilde{x}_i$ and variance $\sigma_{\tilde{x}}^2$. Then Δ defined by the expression:

$$\Delta = t\sqrt{\sigma_x^2 / N},$$

(2.3)

where t is the value according to the Student's distribution for $K-1$ degrees of freedom.

This approach makes it possible to form an expert assessment of existing threats for security components (IS, CS, SI), to take into account their focus on hacking/terminating the functionality of security services. The versatility of the approach lies in the objective assessment of experts' judgments, which makes it possible to use this mathematical apparatus when considering the entire spectrum of threats, their possibility of integration, synergy and hybridity.

To form metric (weight) coefficients of threats (**Fig. 2.3**) and their impact on security services, let's introduce the following designations and offer the following mathematical apparatus:

1. j – security service for CIF. Basic security services:

– C – confidentiality;

– I – integrity;

– A – availability;

– Au – authenticity;

– Aff – involvement (affiliation).

Thus, a vector of security services is formed in the classifier $j = \{C, I, A, Au, Aff\}$.

2. N – the number of threats.

3. K – the number of experts.

4. $\{i\}_1^N$ – thread number of the i-th threat; $\{k\}_1^K$ – the number of the expert.

To assess the hybrid and synergistic components of threats, let's use the following procedure:

Step 1. Threat Relationship Assessment and Security Services:

$$w_j^{CPS\,CIF} = \frac{1}{K} \sum_{i=1}^{N} \sum_{k=1}^{K} w_j^{CPS\,CIF}{}_{ik}, \tag{2.4}$$

where $w_j^{CPS\,CIF}{}_{ik}$ – the value of the coefficient set by the k-th expert for the i-th threat of the j-th security service.

Step 2. Formation of coefficients of threats (proposed in [1, 2]):

$$\alpha_i^{CPS\,CIF}, i \in \left[0.067; 0.133; 0.2; 0.267; 0.333\right].$$

Step 3. Determination of threat realization:

$$w_j^{CPS\,CIF}{}_i P_j^{CPS\,CIF}{}_i = \frac{1}{K} P_j^{CPS\,CIF}{}_i \sum_{k=1}^{N} w_j^{CPS\,CIF}{}_{ik},$$

where

$$P_j^{CPS\,CIF}{}_i \in \left\{\alpha_i^{CPS\,CIF}\right\}. \tag{2.5}$$

For security services and the i-th threat:

$$w_j^{CPS\,CIF\,C}{}_i P_j^{CPS\,CIF\,C}{}_i = \frac{1}{K} P_j^{CPS\,CIF\,C}{}_i \sum_{k=1}^{N} w_j^{CPS\,CIF\,C}{}_{ik},$$

where

$$P_j^{CPS\,CIF\,C}{}_i \in \{\alpha_i^{CPS\,CIF\,C}{}_i\};$$

$$w_j^{CPS\,CIF\,I}{}_i P_j^{CPS\,CIF\,I}{}_i = \frac{1}{K} P_j^{CPS\,CIF\,I}{}_i \sum_{k=1}^{N} w_j^{CPS\,CIF\,I}{}_{ik},$$

where

$$P_j^{CPS\,CIF\,I}{}_i \in \{\alpha_i^{CPS\,CIF\,I}{}_i\};$$

$$w_j^{CPS\,CIF\,A}{}_i P_j^{CPS\,CIF\,A}{}_i = \frac{1}{K} P_j^{CPS\,CIF\,A}{}_i \sum_{k=1}^{N} w_j^{CPS\,CIF\,A}{}_{ik},$$

where

$$P_{j\ \ i}^{CPS\ CIF\ A} \in \left\{ \alpha_{i\ \ i}^{CPS\ CIF\ A} \right\};$$

(2.6)

$$w_{j\ \ i}^{CPS\ CIF\ Au}P_{j\ \ i}^{CPS\ CIF\ Au} = \frac{1}{K}P_{j\ \ i}^{CPS\ CIF\ Au}\sum_{k=1}^{N}w_{j\ \ ik}^{CPS\ CIF\ Au},$$

where

$$P_{j\ \ i}^{CPS\ CIF\ Au} \in \{\alpha_{i\ \ i}^{CPS\ CIF\ Au}\};$$

$$w_{j\ \ i}^{CPS\ CIF\ Aff}P_{j\ \ i}^{CPS\ CIF\ Aff} = \frac{1}{K}P_{j\ \ i}^{CPS\ CIF\ Aff}\sum_{k=1}^{N}w_{j\ \ ik}^{CPS\ CIF\ Aff},$$

where

$$P_{j\ \ i}^{CPS\ CIF\ Aff} \in \left\{ \alpha_{i\ \ i}^{CPS\ CIF\ Aff} \right\},$$

where $w_{j\ \ i}^{CFS\ CIF\ C}$, $w_{j\ \ i}^{CFS\ CIF\ I}$, $w_{j\ \ i}^{CFS\ CIF\ A}$, $w_{j\ \ i}^{CFS\ CIF\ Au}$, $w_{j\ \ i}^{CFS\ CIF\ Aff}$ — weight coefficients of security services: C, I, A, Au, Aff; $\alpha_{\ \ i}^{CPS\ CIF\ C}$, $\alpha_{\ \ i}^{CPS\ CIF\ I}$, $\alpha_{\ \ i}^{CPS\ CIF\ A}$, $\alpha_{\ \ i}^{CPS\ CIF\ Au}$, $\alpha_{\ \ i}^{CPS\ CIF\ Aff}$ — weight coefficients of the security service: C, I, A, Au, Aff manifestations of the attack of the i-th threat.

Step 4. Determination of the implementation of several threats to the security service:

$$W_{synerg}^{CFS\ CIF\ Au} = \sum_{i=1}^{M}w_{synerg\ i}^{CFS\ CIF\ Au}\alpha_{\ \ i}^{CPS\ CIF\ Au}; \quad W_{synerg}^{CFS\ CIF\ C} = \sum_{i=1}^{M}w_{synerg\ i}^{CFS\ CIF\ C}\alpha_{\ \ i}^{CPS\ CIF\ C};$$

$$W_{synerg}^{CFS\ CIF\ I} = \sum_{i=1}^{M}w_{synerg\ i}^{CFS\ CIF\ I}\alpha_{\ \ i}^{CPS\ CIF\ I}; \quad W_{synerg}^{CFS\ CIF\ A} = \sum_{i=1}^{M}w_{synerg\ i}^{CFS\ CIF\ A}\alpha_{\ \ i}^{CPS\ CIF\ A};$$

$$W_{synerg}^{CFS\ CIF\ Aff} = \sum_{i=1}^{M}w_{synerg\ i}^{CFS\ CIF\ Aff}\alpha_{\ \ i}^{CPS\ CIF\ Aff},$$

(2.7)

where M – the number of threats selected by an expert from $\{i\}_{i}^{M}$, $M \leq N$.

When forming the metric coefficients, it is considered that the results obtained refer to independent threats, in the case of their dependence (coincidence of the threat tuples), it is necessary to use the expression for determining the total probability of dependent events:

$$P(AB) = P(A) + P(B) - P(AB).$$

(2.8)

In this case, only tuples of vectors are evaluated that refer to the threats themselves (platforms 1–5). This approach makes it possible, without reference to the categories of critical

infrastructure objects, to form a common unified base of threats for all CIFs that can lead to terrorist attacks, their likelihood of implementation and possible damage.

Step 5. Determination of a synergistic threat by security components:

$$W_{synerg}^{IS} = \sum_{i=1}^{N} \left(\sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ C} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ I} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ A} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Au} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Aff} \right) \alpha_i^{CPS\ CIF},$$

$$W_{synerg}^{CS} = \sum_{i=1}^{N} \left(\sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ C} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ I} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ A} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Au} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Aff} \right) \alpha_i^{CPS\ CIF},$$

$$W_{synerg}^{SI} = \sum_{i=1}^{N} \left(\sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ C} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ I} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ A} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Au} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Aff} \right) \alpha_i^{CPS\ CIF}. \quad (2.9)$$

To determine the total synergistic threat:

$$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \bigcup W_{synerg}^{CS} \bigcup W_{synerg}^{SI}. \quad (2.10)$$

To determine the total hybrid threat:

$$W_{hybrid\ C,I,A,Au,Af\ synerg}^{CPS\ CIF} = W_{synerg}^{CFS\ CIF\ C} \cap W_{synerg}^{CFS\ CIF\ I} \cap W_{synerg}^{CFS\ CIF\ A} \cap W_{synerg}^{CFS\ CIF\ Au} \cap W_{synerg}^{CFS\ CIF\ Aff}. \quad (2.11)$$

Step 6. Minimization of financial costs for preventive protection measures (let's use the procedure proposed in [1, 2]).

Thus, the main difference of the proposed approach is the possibility of forming a single unified base of threats to critical infrastructure facilities regardless of the CIF category. This makes it possible not only to simplify the formation of the threat base on the CIF, but also to timely take into account the vectors of targeted attacks, the possibility of their integration, synergy and hybridity, as well as identify the critical points of the CIF infrastructure, their relationship with information resources. In addition, the proposed approach minimizes funding for the creation of a security loop for CIF business processes, as well as timely formulate preventive measures and protection profiles.

Understanding and mitigating risks and threats to critical infrastructures is highly dependent on the ability to create and validate models, often involving physical systems or even human intervention.

The problem space of modeling includes both critical systems in general, such as industrial process control systems at critical facilities, and interactions between several sectors of critical systems. Such a range of objects can be effectively described only by the same wide range of modeling methods corresponding to the studied aspects of the infrastructure. In many models, the definition of composite OCI was made on the basis of the impact of events or chains of events that affect infrastructure elements. This understanding, in particular of risk at different scales, leads to a classification mechanism originally proposed in [1, 2] in the context of technical risk

modeling and subsequently refined [10] into an infrastructure scale taxonomy, as shown in **Fig. 2.4**. Verifying the applicability of the presented models for safety analysis requires significant effort. This is true even if the model takes into account all parameters related to safety and reliability analysis.
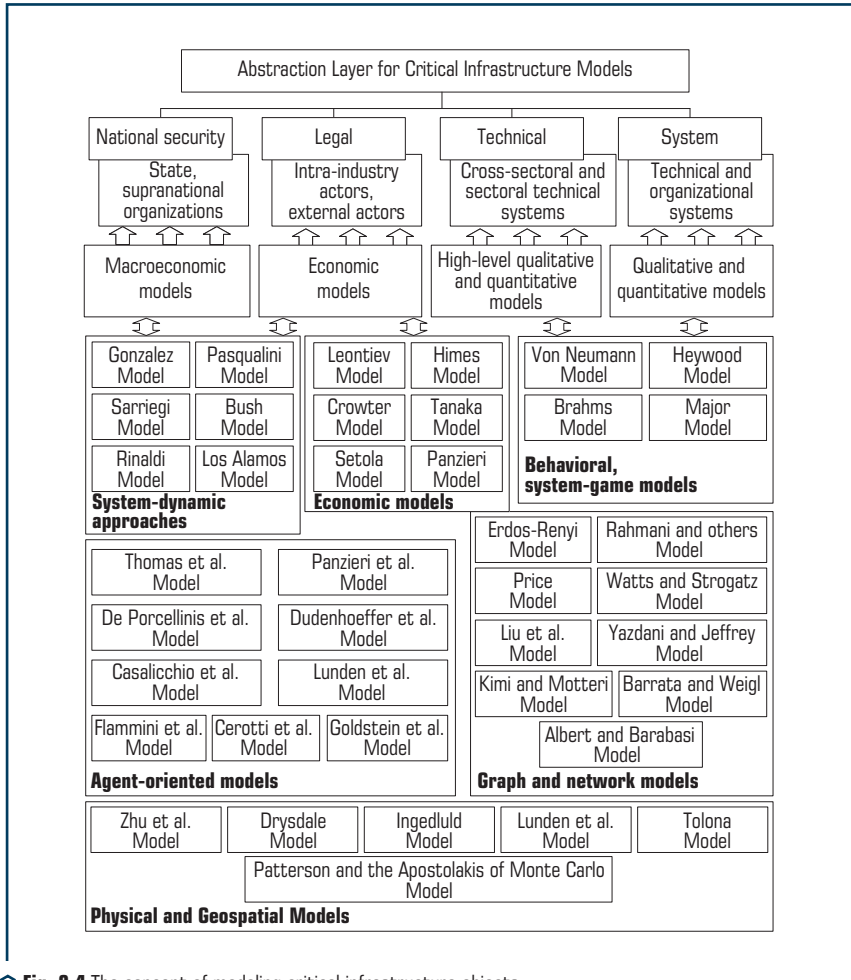
○ **Fig. 2.4** The concept of modeling critical infrastructure objects

For lower levels of abstraction, it may be possible to derive and test such models explicitly from the underlying principles. At higher levels of abstraction, this leads to uncertainty in the validity of the model.

Such uncertainty is already problematic when it is not easy to determine whether the underlying problem itself is ill-conditioned. Conditionality is defined as a situation where small variations in parameters lead to disproportionate changes in results. Bad conditioning can be a feature of the modeling method. This problem also arises in the context of combining several specialized models or models that address different levels of abstraction [11].

Economic models serve mainly to identify high-level dependencies, and can also reveal quantitative effects, albeit with a relatively low resolution. Most of the models used in the area of critical infrastructure are input-output models, focusing primarily on aspects driven by demand or supply. However, such models are necessarily limited to the state of equilibrium.

An application to critical infrastructures was originally proposed in [12], where several interconnected systems are considered, including intra-industry dependencies. The purpose of the review is to identify inoperability caused by one or more failures. Such failures are both natural and can be caused artificially. In the proposed model, inoperability is defined as the level of system dysfunction, i.e., as part of its expected level of performance, which is described by the Inoperability Input-Output model (IIM).

Dynamic IIM allows analysis of parameters such as optimization of buffering in the form of reserves to mitigate fluctuations in supply levels [13]. The use of explicit probabilistic vectors of disturbances from the demand side in IIM increases the reliability of the obtained modeling results and the applicability of the models for cybersecurity purposes [14–16].

Applicability for cybersecurity purposes may require the introduction of its own cost metric for disparate objects included in the critical infrastructure [17–19].

System-dynamic approaches considered in [20–23]. So, at work [20] considered the relationship between infrastructure objects and information flows, the study of the structural properties of CIF in [21, 22]. System dynamics provides insight into the types of threats to critical infrastructure, in particular attacks such as social engineering [23].

Practice shows that it is difficult to avoid internal attacks, including attacks based on social engineering rather than technical measures. Therefore, when designing control mechanisms, it is necessary to focus on the ways in which controls and interactions can cause delays for attackers in realizing their goals.

Behavioral and systemic game models proposed in [24–26]. Such methods are usually based on a combination of expert judgment and Bayesian statistics [24] or based on explicit causal models. This approach may be useless when the adaptability of the intellectual adversary is assumed [25].

Behavioral and game-theoretic models assume the presence of two or more agents whose interactions can be modeled under various constraints [26]. However, these interactions usually include:

– the ability to cooperate or act against the interests of other agents;
– the ability to interact with different levels of information about each other;
– the possibility of both one-time interaction and interaction over several rounds;
– the attainability of agents' solutions both simultaneously and sequentially.

This type of model assumes that agents are rational and act to maximize their utility. This is done by evaluating the results and choosing the actions that give the most preferable results, taking into account the actions of other players.

The use of game-theoretic models to protect critical information infrastructures is not well represented in the literature. Besides [27], examples include the use of stochastic games for two players [28] to capture the behavior of attackers when the Nash equilibrium is reached. The model in [29] attempts to explicitly map the perception of attackers in the game-theoretic structure, as well as parameters, including resource allocation. Many of the problems studied for physical security and counter-terrorism require careful analysis, taking into account various assumptions, which includes modeling of substitutional effects and the amount of mutual information [30]. Existing models [31] and subsequent developments [32, 33], not only estimate the parameters, but also assume the simultaneous play of attackers and defenders [34, 35].

Graphics and network models provide rigorous formalization [36] and are easily adaptable to network infrastructures such as telecommunications, pipelines, and power distribution. By assigning a set of properties to nodes and edges and by defining flows along the edges of a graph, it is possible to cover many aspects of critical infrastructures and their relationships for both physical assets and information flows. One of the main goals of such models is usually to capture the physical and logical dependencies between network components, which themselves may belong to several different infrastructure sectors.

Critical infrastructures are often long, and individual infrastructures can contain more than 10^5 elements. This explains the interest in studying graphical concepts to understand how graph or interaction structures can be used to characterize the resilience of a network infrastructure.

Particular attention should be paid to the intensive study of random graphs such as the Erdös-Renyi graphs [36, 37].

Empirical research has shown that many networks, both in nature and created by humans, are inherently scaleless. To reflect the dynamics of the critical infrastructure, the processes of graph growth and the mechanism of preferential joining of new edges added to the graph are considered [38]. This work has resulted in a number of techniques more widely used in statistical mechanics being applied to complex networks, including critical infrastructures and their dependencies [39, 40]. Review [41] provides a broader view of complex networks in general.

Agent models are often used in the analysis of infrastructure interdependencies. Infrastructures or physical components are modeled as agents, which allows analysis of the performance and physical condition of the infrastructure, but also provides the ability to capture behavioral aspects, including irrational behavior [41]. Such agent-based systems have been widely used in other fields, which has made it possible to use the results obtained to capture aspects such as the interaction of physical objects [42]. In the model of interacting social agents, descriptions of the interaction of physical agents were integrated, for example, to track the behavior of agents in the electricity and natural gas markets [42].

Physical and Geospatial Models usually designed to solve well-defined problems in a particular sector or for a specific facility. These models exhibit high computational complexity, while significantly varying the level of detail provided [20] from simple vulnerability analysis and intra-industry dependencies to continuous physical models.

Such models are necessary to describe the internal workings of infrastructures [43], which allows for quantitative risk analysis [44]. External influences on critical infrastructures, such as cyberattacks, must be taken into account and even generated in the model. Spatial proximity is an important parameter in the study of interdependencies and physical effects, which is not always clear from the analysis of only logical dependencies. Therefore, a number of efforts have been aimed at creating models of critical infrastructures and their interdependencies based on geospatial information systems (GIS) [45, 46]. Examples of the use of GIS functions in the area of critical infrastructure include approaches based on the theory of multi-attribute utility for forecasting.

2.2 DEVELOPMENT OF A MODEL FOR THE IMPLEMENTATION OF A TERRORIST ACT AND THE DEGREE OF SECURITY OF THE CYBER SYSTEM OF A CRITICAL INFRASTRUCTURE OBJECT

The formation of a complex (echelon) protection of a critical infrastructure object is formed on the basis of the hierarchical structure of the synthesis of information security systems of cyber-physical systems, Internet technologies and computer networks, as well as mobile technologies. This approach makes it possible to form a synergistic model of threats to CIF, taking into account the impact of terrorists on its elements (**Fig. 2.5**).

To form a model for the implementation of a terrorist act and the degree of security of the cyber system of a critical infrastructure object, a mathematical apparatus has been developed:

— classification allows to enter elements of many categories of intruders $L_i^{del} \in \{L^{del}\}$: L_1^{del} — CIF users; L_2^{del} — CIF operating personnel; L_3^{del} — technical support staff of the CIF; L_4^{del} — persons who are not employees of the CIF; L_5^{del} — terrorists and perpetrators of terrorist acts: L_{51}^{del} — cyber terrorists, L_{41}^{del} — special services, L_{52}^{del} — hackers, L_{42}^{del} — competitors, L_{53}^{del} — crime, L_{54}^{del} — vandals;

— define the model for the implementation of a terrorist act:

$$G_{terror}^{CFS\,CIF} = \left\{ L_i^{del}, \beta_i^{CPS\,CIF} \in \left\{ \beta_{terror}^{CPS\,CIF} \right\}, p_{rj}, r_{motiv}, T \right\}, \tag{2.12}$$

where $L_i^{del} \in \{L_i^{del}\}$ — identifier of the terrorist executor; $\beta_i^{CPS\,CIF} \in \{\beta_{terror}^{CPS\,CIF}\}$ — the weighting coefficient of the capabilities of the terrorist executing the terrorist attack on the OKI; T — time of successful implementation of the threat; p_{rj} — the probability of realization of at least one threat to the j-th asset, i — the threat, $\forall i \in n$, n — the number of threats; j — information resource (asset); $\forall j \in m$, m — the number of assets; r_{motiv} — stimulation of the terrorist executor to carry out a terrorist attack on the CIF; T — the time of the attack Analysis of the categories of attackers allows

to form an expert assessment and obtain a weighting coefficient for the possibility of implementing threats (the *i*-th threat);

— the weighting coefficient of the terrorist-performer's capabilities is determined by:

$$\gamma_{terror}^{CPS\ CIF} = \frac{1}{N}\sum_{i=1}^{N}\beta_i^{CPS\ CIF} \times p_{rj} \times r_{motiv},$$ (2.13)

where $\beta_i^{CPS\ CIF} = W_{cp}^{CPS\ CIF} \bigcap W_{cash}^{CPS\ CIF} \bigcap T$ — weighting coefficients of the terrorist-performer's capabilities; $W_{cp}^{CPS\ CIF}$ — computing resources of the terrorist-performer use from [1, 2]); $W_{cash}^{CPS\ CIF}$ — financial resources of the terrorist-executor (use from [1, 2]).
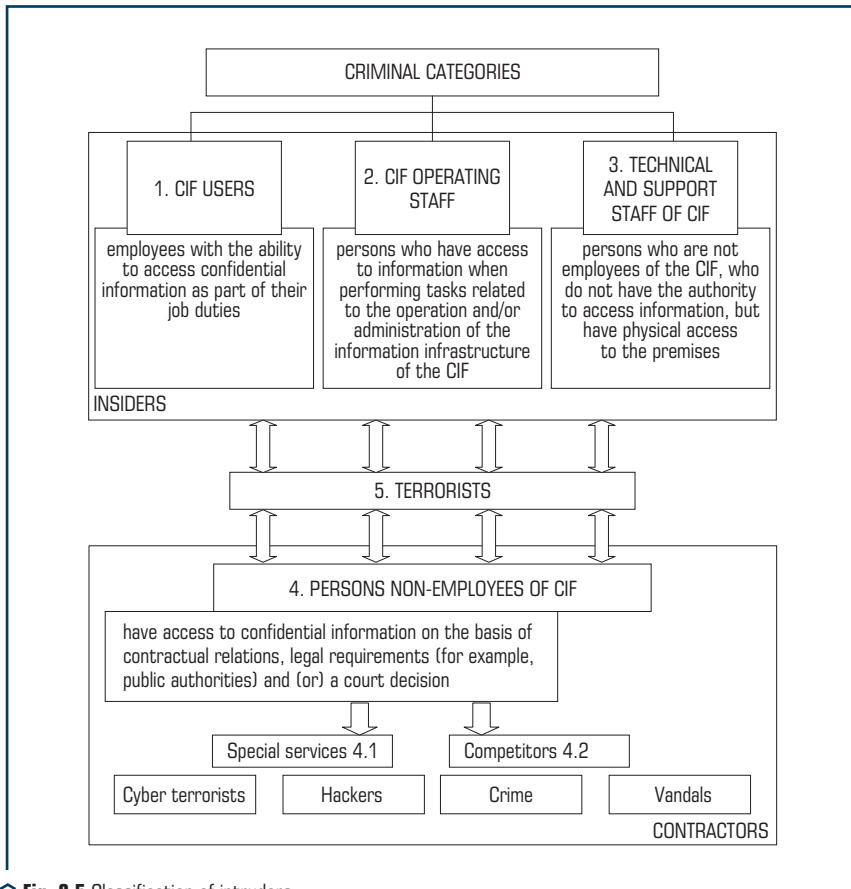
Fig. 2.5 Classification of intruders

The proposed approach makes it possible to unify the procedure for determining the likelihood of a terrorist attack on the CIF, taking into account the capabilities of the terrorist perpetrator, both financial and computing resources.

The analysis of the level of the infrastructure of the CIF and the categories of the terrorist-perpetrator makes it possible to form the set $\{H_j\}$, which forms the levels of impact on the CIF: the level of technical channels (H_0); physical layer ISO/OSI (H_1); link layer ISO/OSI (H_2); network layer ISO/OSI (H_3); transport layer ISO/OSI (H_4); ISO/OSI application layer (H_5); the level of physical protection of the CIF elements (video surveillance, sensors, grilles, locks, etc.) (H_6); level of possible embedded devices (ventilation ducts, power lines, etc.) (H_7).

The matrix of the relationship between the category of the terrorist-performer and the level of impact on the CIF is defined.

Thus, the matrix of interaction between the categories of the terrorist-executor and the levels of impact on the CIF makes it possible to determine the category of the terrorist-executor according to the threat classifier according to the proposed method:

– Stage 1. Determination of the level of impact on the CIF from the set $\{H\}$;

– Stage 2. Definition of the threat according to the CIF threat classifier;

– Stage 3. Determination of the matrix of the relationship between the category of the terrorist-performer and the level of impact on the CIF;

– Stage 4. Determination of a possible terrorist perpetrator from the interconnection matrix.

$$M_{L_i^{del}}^{H_i} = \left\| L_i^{del} \right\| \times \left\| H_i \right\| = \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}. \qquad (2.14)$$

Thus, on the basis of the proposed methodology, a list of critical threats for each category of violators is constructed. Taking into account the modern approaches proposed in [47–52] for assessing the level of possible embedded devices (H_7), the time and financial costs for preventive measures of protection are significantly reduced.

2.3 DEVELOPMENT OF A CONCEPT FOR ASSESSING THE LEVEL OF SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES

To determine the current state of security, let's use the approach proposed in [1, 2], which takes into account the proposed approach to the formation of a synergistic threat model, the category of attackers, their goals and capabilities. **Fig. 2.6** shows the concept of assessing the level of protection of critical infrastructure facilities.

Advanced Threat Classifier
generalized synergistic threat

$$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \bigcup W_{synerg}^{CS} \bigcup W_{synerg}^{SI}$$

given its hybridity

$$W_{hybrid\ C,I,A,Au,Af\ synerg}^{CPS\ CIF} = W_{synerg}^{CFS\ CIF\ C} \bigcap W_{synerg}^{CFS\ CIF\ I} \bigcap W_{synerg}^{CFS\ CIF\ A} \bigcap W_{synerg}^{CFS\ CIF\ Au} \bigcap W_{synerg}^{CFS\ CIF\ Aff}$$

Advanced CIF Infrastructure Model

$$G^{CIF} = \{\{O^{CIF}\}, \{L^{CIF}\}, \{I_A\}\}$$

Synergetic threats model

$$SM_{synerg}^{CIF} = \left\{ \begin{array}{l} \{SS_{threats}^{CIF}\}, \{\alpha_i^{CPS\ CIF}\}, \\ \{W_{synerg\ i}^{CFS\ CIF}\}, \{G_{terror}^{CFS\ CIF}\}, \{DS\} \end{array} \right\}$$

Evaluation of security of information in the CPS CIF

Terrorist attack model

$$MT_{terror}^{CIF} = \left\{ \begin{array}{l} L^{del}, p_{rj}, target, T, \\ D_{potential}, r_{motiv}, risk \end{array} \right\}$$

Improved security assessment model

$$MT_{terror}^{CIF} = \left\{ \begin{array}{l} \{I_A\}, \{O^{CIF}\}, \{SS_{threats}^{CIF}\}, \\ \{RR^{CIF}\}, \{MP^{CIF}\}, \\ \{AD^{CIF}\}, \{SL_r^{CIF}\} \end{array} \right\},$$

Value of the generalized indicator of the level of security of the CIF

$$OPZ^{CIF} = \sum_{i=1}^{k} OPZ_i$$

$$SL^{CIF} = \left\{ \begin{array}{l} \text{tall, if } OPZ^{CIF} = 4; \\ \text{average, if } 2 \leq OPZ^{CIF} \leq 3; \\ \text{low, if } OPZ^{CIF} = 1; \\ \text{critical, if } OPZ^{CIF} = 0 \end{array} \right.$$

Fig. 2.6 CIF security assessment concept

To form an assessment of the current state, it is proposed to use the following mathematical apparatus:

— the formally improved model of the CIF infrastructure is defined:

$$G^{CIF} = \{\{O^{CIF}\}, \{L^{CIF}\}, \{I_A\}\}, \tag{2.15}$$

where $\{O^{CIF}\}$ — a set of environment objects that describe the elements of the CIF infrastructure; $\{L^{CIF}\}$ — a set of links between elements, defined by an adjacency matrix; $\{I_A\}$ — many elements of information assets.

Each element $I_{A_i} \in \{I_A\}$ described by the vector $I_{A_i} = (Type, A^C, A^I, A^A, A^{Au}, A^{Aff}, A^{cont})$. $Type$ — type of information asset, described by a set of basic values: $Type = \{CI, PD, CD, TS, StR, Publ, Contl, PI\}$, where CI — confidential information, PD — payment documents, CD — credit documents, TS — trade secret, StR — statistical reports, $Publ$ — public information, $Contl$ — control information, PI — personal data. $AC, AI, AA, AAu, AAff, Acont$ — security services.

Each element $O_i^{CIF} \in \{O^{CIF}\}$, described by the vector $O_i^{CIF} = \{L^{CIF}, TC^{CIF}\}$, where L^{CIF} is the level of the CIF information structure, defined by the set $L^{CIF} = \{H_0, H_1, H_2, H_3, H_4, H_5, H_6, H_7\}$, where the level of technical channels (H_0), physical layer ISO/OSI (H_1), data link layer (H_2), network layer (H_3), transport layer (H_4), application layer (H_5), physical protection level of CPS CIF elements (H_6), the level of possible embedded devices (H_7);

— formally, the relationship between the IR and the elements of the CIF:

$$TC^{CIF} = \left\| TC_{il}^{CIF} \right\|, \tag{2.16}$$

where TC_{il}^{CIF} determines the relationship between the i-th IR and the l-th element of the CIF, while:

$$\forall i \in \{I_A\}, \forall l \in \{O^{CIF}\} \Rightarrow TC_{il}^{CIF} = \begin{cases} 0, \text{ no connection;} \\ is, \text{ includes and stores;} \\ pt, \text{ processes and transfers;} \\ mf, \text{ maintains the functioning;} \end{cases} \tag{2.17}$$

— the proposed synergistic model of threats to the CIF:

$$SM_{synerg}^{CIF} = \left\{ \{SS_{threats}^{CIF}\}, \{\alpha_i^{CPS\ CIF}\}, \{W_{synerg\ i}^{CFS\ CIF}\}, \{G_{terror}^{CFS\ CIF}\}, \{DS\} \right\}, \tag{2.18}$$

where $SS_{threats}^{CIF} = \{\{SS_{MMS}^{CIF}\}, \{AS_{threats}^{CIF}\}\}$ — many possible threats, in which $\{SS_{MMS}^{CIF}\}$ — man-made threats; $SS_{MMS}^{CIF} = \{\{SS_{IS}^{CIF}\}, \{SS_{CS}^{CIF}\}, \{SS_{SI}^{CIF}\}\}$ — anthropogenic threats. It is proposed to consider many anthropogenic threats based on a synergetic approach in terms of security components.

Wherein $\{SS_{IS}^{CIF}\}$ — IS threats, $\{SS_{CS}^{CIF}\}$ — CS threats, $\{SS_{SI}^{CIF}\}$ — SI threats; $\{\alpha_i^{CPS\,CIF}\}$ — a set of threat weights; $\{W_{synerg\ i}^{CFS\,CIF}\}$ — many threats to the security service; $\{G_{terror}^{CFS\,CIF}\}$ — a lot of damage from a terrorist attack; $\{DS\}$ — a set of destructive states of CIF elements, which mean complete destruction of CIF (O1), destruction of individual CIF elements (O2), complete blocking of CIF functionality (O3), partial blocking of functionality (O4);

— synergistic effect of modern threats:

$$SS_{threats}^{CIF} = \left\{SS_{MMS}^{CIF}\right\} \cup \left\{AS_{threats}^{CIF}\right\},$$

where

$$SS_{MMS}^{CIF} = \left\{SS_{IS}^{CIF}\right\} \cap \left\{SS_{CS}^{CIF}\right\} \cap \left\{SS_{SI}^{CIF}\right\}. \tag{2.19}$$

— each threat to the elements of the CIF is formalized by a tuple:

$$SS_{threats}^{CIF} = \left(p_{rj}, D_{potential}, risk\right), \tag{2.20}$$

where p_{rj} — the probability of a threat to the j-th asset, i — threat, for all i that belong to n — the number of threats, j — IR (asset), for all j that belong to m — the number of IR; $D_{potential}$ — potential damage, $risk$ — risk expressed in a qualitative form and taking one of the values $risk = (\alpha_{r_1}, \alpha_{r_2}, \alpha_{r_3}, \alpha_{r_4}, \alpha_{r_5})$, where α_{r_1} — critical, α_{r_2} — tall, α_{r_3} — middle, α_{r_4} — low, α_{r_5} — very low;

— destructive states of CIF elements (set $\{DS\}$) let's use from [1, 2]. Let's define the formal model of the terrorist performer:

$$MT_{terror}^{CIF} = \left\{\left\{L^{del}, p_{rj}, target, T, D_{potential}, r_{motiv}, risk\right\}\right\}, \tag{2.21}$$

where L_{del} — categories of intruders; $target$ — the target of the attacker, $target \in \{DS\}$; T — time of successful implementation of the threat; r_{motiv} — the probability of the terrorist executor's incentive.

— formally, the links between the categories of violators and the levels of their impact on the CIF elements are set by the matrix $CT_{impact}^{CIF} = \left\|a_{ij}^{CIF}\right\|$, wherein $a_{ij}^{CIF} = 1$, if the source of threats $SS_{threats}^{CIF}$ can implement a threat against the j-th CIF asset $O_l^{CIF} \in \{O^{CIF}\}$, otherwise $a_{ij}^{CIF} = 0$.

— CIF security assessment model:

$$MT_{terror}^{CIF} = \left\{\{I_A\}, \{O^{CIF}\}, \{SS_{threats}^{CIF}\}, \{RR^{CIF}\}, \{MP^{CIF}\}, \{AD^{CIF}\}, \{SL_r^{CIF}\}\right\}, \tag{2.22}$$

where $\{I_A\}$ — a lot of IRs; $\{O^{CIF}\}$ — a lot of elements of the CIF infrastructure; $\{SS_{threats}^{CIF}\}$ — many threats; $\{RR^{CIF}\}$ — many requirements of IS regulators; $\{MP^{CIF}\}$ — many elements of information security; $\{AD^{CIF}\}$ — result of CIF security assessment; $\{SL_r^{CIF}\}$ — CIF security level;

– formally, the relationship between threats and IR:

$$TI^{CIF} = \left\| \beta_{ij}^{CIF} \right\|, \forall j \in \{I_A\}, \forall i \in \left\{ SS_{threats\,i}^{CIF} \right\}, \tag{2.23}$$

where 1 – the threat exists for the IR, 0 – the threat does not exist for the IR;
– the protection mechanism is formed by a tuple:

$$MP^{CIF}_{\ i} = \left(T_{pe}, T_{introducing}, C_{pe} \right), \tag{2.24}$$

where T_{pe} – the type of the GI tool; $T_{introducing}$ – the implementation time; C_{pe} – the cost of the GI tool;
– formally, the relationship between threats and information security systems:

$$L_{ThIS}^{CIF} = \left\| \gamma_{ij}^{ThIS} \right\|, \tag{2.25}$$

where MP^{CIF} – the threat can be repelled by the ISS; NMP^{CIF} – the threat is being realized.
If a $\lambda_{ij}^{LThIS} = NMP^{CIF}$, it is concluded that the CIF SIS is not able to protect the IR from the threat, and to increase the level of CIF security, it is necessary to introduce additional means and protection mechanisms;
– requirements of international and national standards and legislative acts:

$$\left\{ RR^{CIF} \right\} = \left\{ R_{INS}^{CIF} \right\} \cup \left\{ A_{DSR}^{CIF} \right\}, \tag{2.26}$$

where $\{R_{INS}^{CIF}\}$ – requirements of international and national regulators; $\{A_{DSR}^{CIF}\}$ – a lot of assessments of the degree of implementation of information security.
The current state of the CIF IS will be determined on the basis of the following indicators:
– OPZ_{one} – assessment of the risks of threats and the presence of critical points in the elements of the CIF;
– OPZ_2 – assessment of possible attacks on the elements of the infrastructure of the CIF;
– OPZ_3 – assessment of compliance with regulatory requirements.

$$OPZ^{CIF} = \sum_{i=1}^{k} OPZ_i. \tag{2.27}$$

The proposed mathematical apparatus of the concept of assessing the level of security of critical infrastructure facilities allows obtaining a qualitative assessment of their current state of information security:

$$SL^{CIF} = \begin{cases} \text{tall, if } OPZ^{CIF} = 4; \\ \text{average, if } 2 \leq OPZ^{CIF} \leq 3; \\ \text{low, if } OPZ^{CIF} = 1; \\ \text{critical, if } OPZ^{CIF} = 0. \end{cases}$$

(2.28)

Thus, the proposed approach is understandable to the average person, it allows one to intuitively understand the main critical points of the CIF infrastructure, the possibility of carrying out a terrorist attack on quiet, as well as the necessary preventive measures, in conditions of minimizing the financial security of the information security system.

2.4 DEVELOPMENT OF A METHOD FOR ASSESSING THE SECURITY OF CYBER-PHYSICAL SYSTEMS BASED ON THE LOTKA-VOLTERRA MODEL

To assess the security of cyber-physical systems under the influence of modern targeted cyber threats with signs of hybridity and synergy, their integration with social engineering methods on infrastructure elements is taken into account. At the same time, the classical Lotka-Volterra model uses the main approaches based on the following paradigms:
– in the absence of «predators», «prey» multiply exponentially;
– in the absence of «prey», «predators» die out exponentially.

At the same time, as a rule, in works [1, 2, 47–51], within the framework of the «prey», IS incidents/attackers are considered, and the «predator» is the protection measures/elements of the protection system. This looks illogical from the point of view of the ecosystem, which means cyberspace. Mathematically, the «predator-prey» model can be described as [47]:

$$\begin{cases} \dfrac{dN_1}{dt} = \alpha N_1 - \beta N_1 N_2; \\ \dfrac{dN_2}{dt} = -\varphi N_2 + \gamma N_2 N_1, \end{cases}$$

(2.29)

where N_1 – the number of prey; N_2 – the number of predators; α – the fertility rate of prey; β – the coefficient of the influence of the predator on the prey (the coefficient of predation); φ – the coefficient of mortality of the predator; γ – the coefficient of the influence of the prey on the predator.

Fig. 2.7 shows the relationship of the proposed definitions. The main difference from known approaches is the ability to take into account not only the aggregation of threats, the formation of targeted attacks, but also their impact on individual security components. This approach provides the granularity of today's threats, and makes it easier to understand their impact on the level of security in general.
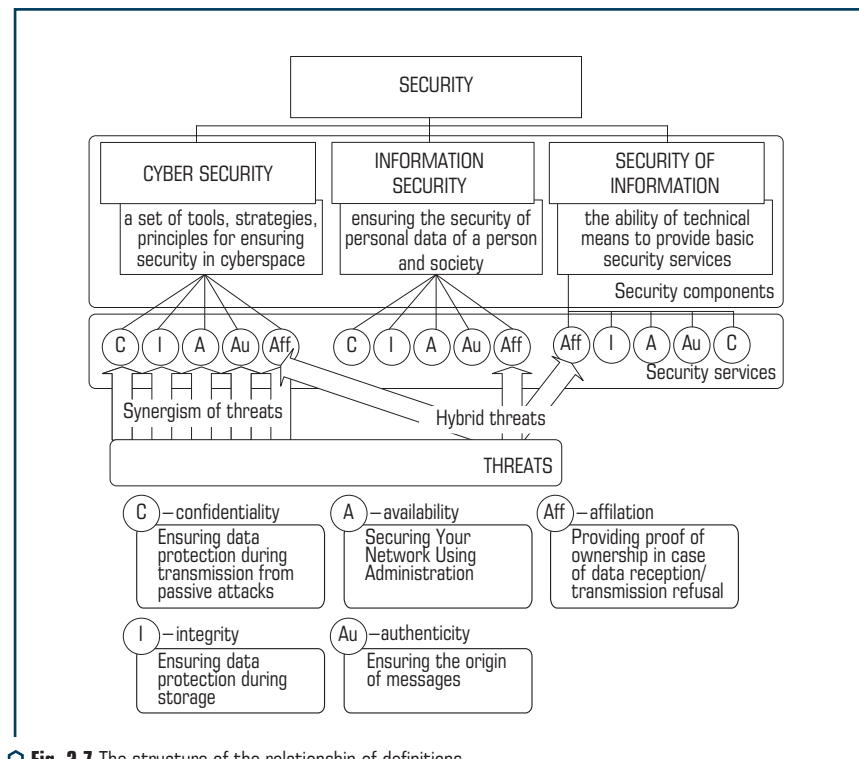
○ **Fig. 2.7** The structure of the relationship of definitions

However, to assess the security of cyber-physical systems, it is proposed to use the following concepts:

– «prey» – a system or element of a system/infrastructure of an information and communication system/cyber-physical system that is subject to targeted threats with signs of synergy and hybridity;

– «predator» – a target threat or threat to separate components of security (cybersecurity (CS), information security (IS), security of information (SI)) on a system or element of a system/infrastructure of an information and communication system/cyberphysical system or Internet of Things system;

– security of information resources (IR) – the state of security of IR, characterized by the ability of users, technical means and information technologies to ensure confidentiality, integrity, authenticity and availability when processing them in ICS with IoTS;

– cybersecurity of IR (CS IR) – a set of tools, strategies, principles of security, security guarantees, approaches to risk management, actions, training, insurance and technologies that are used to protect the cybersecurity of ICS from IoTS, resources and users of cyberphysical systems;

– information security of IR (IS IR) – the state of security of the information environment of ICS with IoTS, ensuring its formation, use and development in the interests of citizens and ICS with IoTS;

– the hybridity of IS, CS, SI threats – a set of several threats to information resources by security components: information security, cybersecurity, security of information, aimed at a separate security service: confidentiality, integrity or authenticity. This allows to get the maximum effect from their integration;

– synergism of IS, CS, SI threats – the combined impact of several threats on security components: information security, cyber security, information security with security services: confidentiality, integrity, authenticity. It is characterized by the fact that their combined effect significantly exceeds the effect of each individual threat and their simple sum;

– emergence of ICS/CPS – a set of special properties of ICS/CPS that do not belong to its subsystems and blocks, as well as the sum of elements that are not connected by special system-forming links. Based on the assessment of the synergy and hybridity of threats to security components, the costs of investing in building a security system are minimized to ensure the efficiency and reliability of information transfer;

– the level of security of information resources – a qualitative (quantitative) indicator of the ability of the ICS/CPS protection system to resist synergistic and hybrid threats to security components: information security, cybersecurity, security of information;

– business-processes continuity – a property of the system, which is to ensure the uninterrupted operation of internal and external applications, which allows subsystems and services to work without interruption during planned downtime and unplanned failures. It also ensures that critical business data is backed up and stored and can be restored within a reasonable period of time in the event of an unexpected incident or disaster;

– the security loop of business processes – the minimum permissible set of means of protecting the aggregate of information resources and related business processes. The execution of business processes in a given sequence leads to the achievement of the goals of the organization.

Development of security models for developing cyber-physical systems, taking into account the computing capabilities and focus of targeted cyberattacks.

To use the «predator – prey» model for modeling the dynamics of functioning and assessing cyber-physical systems, it is necessary not only to give a substantive interpretation of the basic model in terms and concepts of a security system, but also to parameterize the model. In other words, it is necessary to determine the values of the coefficients included in the model equations, as well as to set the initial values of the studied variables.

Let's begin the parametrization of the model with its first equation.

Let's estimate the number of protection elements of the business continuity security loop based on the following assumptions:

1. Threats are aimed at the corresponding security services, which are represented by the 3rd platform in the threat classifier [2, 47].

2. For each of the security services in the security loop, there are facilities that provide those services. The distribution of these funds over the considered range of services is described by a vector $(A_i^C, A_i^I, A_i^A, A_i^{Au}, A_i^{Aff})$. In this case, the equality holds $\sum_{i=1}^{j} A_i^j = 1$, where j — the security services, i — the threat to the elements of the CPS infrastructure.

3. A threat is considered hybrid if it simultaneously targets all security services.

The number of objects representing the targets of attacks, taking into account their hybridity, can be represented as follows:

$$\tilde{N}_1 = \sum_{i=1}^{Q} \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right), \quad (2.30)$$

where variable indices correspond to basic security services: C — confidentiality; I — integrity; A — availability; Au — authenticity; Aff — affiliation; $N_{1_i}^C$ — the number of objects providing security service, such as confidentiality; for other security services — the same; Q — the total number of known cyber threats.

Let's assume that the coefficient of the introduction of new elements of the information security system α corresponds to the level of security of the elements that provide security services for the CFS. The security level, according to [1, 2, 47], is assessed in relative units: 1 — corresponds to the maximum-security level provided by the security system, 0 — the security system does not protect information resources.

Let's assume that the cost of carrying out attacks and the cost of measures to protect against them have a normal distribution. In this case, the probability of the threat being realized with the maximum capabilities of defense A and attack B will be determined by the difference between the probability densities $F(B)–F(A)$, where A are the limiting defense capabilities, B are the limiting capabilities of the attacking side's attack. In other words, $F(B)$ determines the proportion of attacks out of their total number that can be carried out by an attacker based on the resources they have. Similarly, $F(A)$ determines the proportion of attacks that a security system can protect against, based on the resources available to it. Under these assumptions, the value $S=F(B)–F(A)$ determines the proportion of unprotected targets that can be targeted by cyberattacks. Then the level of security will be defined as the proportion of information resources that are protected from cyberattacks. This value can be calculated as:

$$S = 1 - F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} dt, \quad (2.31)$$

where S — the security level of the system, $F(B)$ and $F(A)$ are the shares of resources of the parties to the cyber conflict, t — the integration variable that determines the level of available resources of the «predator» and «prey», μ and σ — the values that determine the mathematical expectation and variance the statistical distribution of the resources available to the parties.

The introduction of cost indicators of threats makes it possible to implement an algorithm for constructing a rating of potential threats and the importance of information resources to be protected.

When implementing the algorithm, it is assumed that the parties to the conflict determine the criticality of cyber threats, which are economically feasible to carry out and/or from which it is necessary to protect the IR in the first place. Then let's define the algorithm:

1st step. Definition of cyber threats, the effect of the implementation of which exceeds the cost of their implementation:

$$Tr_R^A = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \forall Tr_i \in Tr,$$

(2.32)

where Tr_R^A – the set of potential threats, the implementation of which is effective for the attacker; Tr_i – threat to the i-th information resource; P_i^A – estimation of the cost of the successful implementation of an attack on the i-th resource from the side of the attacker; C_i^A – the cost of carrying out an attack on the i-th resource by the attacker.

2nd step. Determination of the direction of protection that provides the effect The assessment of the limit levels of the capabilities of the parties to a cyber conflict is based on the use of cost estimates of the costs of implementing and preventing the threat, as well as on the assessment of the benefits derived from the implementation of the threat and its prevention [2, 47] higher than the cost of their provision:

$$Tr_C^D = \left\{ Tr_j \mid \left(P_i^D - C_i^D \right) > 0 \right\} \forall Tr_j \in Tr,$$

(2.33)

where Tr_C^D – the set of threats against which it is economically expedient to build protection; P_i^D – estimation of the cost of the loss of the i-th information resource for the defense side; $P = C$ – the cost of protecting the i-th information resource for the side of the defense.

3rd step. Determination of the coefficients of importance for the attackers. They are defined as the share of the gain from the total amount of gain that can be obtained potentially when the entire complex of threats for the attackers is realized:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum\limits_{i=1}^{M} \left(P_i^A - C_i^A \right)}, \forall Tr_i \in Tr_R^A, M = \left| Tr_R^A \right|,$$

(2.34)

where K_i^A – the rating coefficient (importance) of the implementation of the threat to the i-th information resource; M – the cardinality of the set of selected potentially effective threats for the attacking side.

4th step. Determination of the coefficients of importance for the defenders. It is defined as the share of the gain from the total amount of the gain, which can be obtained potentially during the implementation of the entire complex of protective measures:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)} \ , \forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|, \tag{2.35}$$

where K_j^D – the rating coefficient (importance) of building the protection of the j-th information resource.

5th step. Selection of critical threats for which, based on the assessment, the product of the attacker's and defender's importance coefficients is maximal:

$$Tr_l = \arg \max_{\forall Tr_j \in Tr_C^D} K_l^D \cdot K_l^A . \tag{2.36}$$

Then the birth rate of «preys» is proposed to be calculated as:

$$\alpha = \frac{\left|\left\{Tr_l\right\}\right|}{Q}, \tag{2.37}$$

where $\left|\left\{Tr_l\right\}\right|$ – the set of critical cyber threats for which there are no means of protection in the information security system (ISS) or they are partially available, but the implementation of the threat can lead to significant and/or critical destruction of the security loop; Q – the total number of known cyber threats.

The coefficient obtained in this way provides management's understanding of the need to install additional means of protection against identified critical attacks.

The equation for the change in the number of modern threats to the CFS with IoTS is presented as a set of threats to the CFS, taking into account the possibility of their signs of synergy and hybridity:

$$\tilde{N}_2 = N_2 \times \left|\left\{W_{hybrid\ C,I,A,Au,Af}\right\}\right|_{synerg}, \tag{2.38}$$

where $\left|\left\{W_{hybrid\ C,I,A,Au,Af}\right\}\right|_{synerg}$ – the power of the set of hybrid threats (i.e., their number), and $\left\{W_{hybrid\ C,I,A,Au,Af}\right\}_{synerg}$ – the set of hybrid threats, which, according to the accepted assumption, are defined as a set of threats simultaneously for all security services. The calculation of individual components is given in [2, 47].

To assess the impact of modern threats on the means of protection, let's use the expression in [2, 47], then the coefficient β is represented as:

$$\beta = \sum_{i=1}^{M}\left(w_{CPSi}^{\ C} \cap w_{CPSi}^{\ I} \cap w_{CPSi}^{\ A} \cap w_{CPSi}^{\ Au} \cap w_{CPSi}^{\ Aff}\right)\chi_i^{CPS}, \tag{2.39}$$

where M – the number of threats that are selected by an expert from a set $\{i\}_i^M$, that is a subset of the entire set of threats of the classifier, that is, $M \le Q$. w_{CPSi}^C, w_{CPSi}^I, w_{CPSi}^A, w_{CPSi}^{Au}, w_{CPSi}^{Aff} – the expert weights of security services: confidentiality, integrity, availability, authenticity and involvement;

χ_i^{CPS} – the weighting factor of security services: confidentiality, integrity, availability, authenticity and authenticity of the manifestation of the attack of the i-th threat.

To determine the coefficient of the computational capabilities of the attacker φ, let's use the classification of attackers, as presented in [2, 47], and represent it as:

$$\varphi = \frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv}, \tag{2.40}$$

where $\nu_i = W_{cp}^{CPS} \cap W_{cash}^{CPS} \cap T$ – attacker opportunity weights; p_{rj} – probability of realization of at least one threat to the j-th asset, i – a threat, $\forall i \in n$, n – the number of threats, j – information resource (asset), $\forall j \in m$, m – the number of assets; r_{motiv} – the probability of the attacker's motivation to implement the threat; W_{cp}^{CPS} – the computational resources of the attacker (used from [51]); W_{cash}^{CPS} – the attacker's financial resources (use from [51]).

Table 2.3 shows the initial data of the criteria and indicators of the expert assessment of its finding.

● **Table 2.3** Initial data of the criteria and indicators of the expert assessment of the weight coefficient of the attacker's computational capabilities

Category	weighting factor $\beta_i^{CPS} \in \{\beta_i^{CPS}\}$			p_{rj}	r_{motiv}
	$f(N) = r + \|A\| \times N$	T^{CPS}	$\|A\|$		
critical	1	1	1	1	1
high	0.75	0.75	0.75	0.75	0.75
average	0.5	0.5	0.5	0.5	0.5
low	0.25	0.25	0.25	0.25	0.25
very low	0.001	0.001	0.001	0.001	0.001

The coefficient of the possibility of preventive measures is presented as:

$$
\begin{cases}
\dfrac{dN_1}{dt} = \left(\arg\max_{\forall Tr_j \in Tr_C^D} K_l^D \times K_l^A \right) \left(\sum_{i=1}^{Q} \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\[2ex]
- \left(\sum_{i=1}^{M} \left(w_{CPSi}^C \cap w_{CPSi}^I \cap w_{CPSi}^A \cap w_{CPSi}^{Au} \cap w_{CPSi}^{Aff} \right) \chi_i^{CPS} \right) \tilde{N}_1 \left(\sum_{j=1}^{w} \tilde{N}_2^w \right) - \varepsilon \tilde{N}_2^2; \\[2ex]
\dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\sum_{j=1}^{w} \tilde{N}_2^w \right) + \\[2ex]
+ \left(\dfrac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \left(\sum_{j=1}^{w} \tilde{N}_2^w \right) \tilde{N}_1 - \xi \tilde{N}_2^2,
\end{cases}
\tag{2.41}
$$

where μ_{kg}^{j} – the weighting coefficient of the g-th metric of the j-th security service for the k-th expert. Normalization of weight coefficients: $\Delta t_{[i-q]}(t) = K/l(t)$, w_{kg}^{j} – the value of the assessment of the g-th characteristic of the information security tool mechanism by the k-th expert for the j-th security service in the case when the degree of security of the system and the destructive actions of attackers are independent. Wherein $B = \{cryptographic\ resistance\ (C_r),\ Key\ data\ amount,\ S_c,\ encryption/decryption\ of\ data\ complexity,\ O_E\}$. Thus, there are a set of characteristics of technical means of information security: $\mu^{j} = \left|\{C_r^{j}, S_c^{j}, O_E^{j}\}\right|$, $\mu^{j} = \{C_r^{j}, S_c, O_E\}$, which corresponds to the level of security of cryptographic means of information security. To describe the set of characteristics, let's use the index g: μ_g, where $(\{g\}_1^B)$.

Thus, using the obtained expressions, the Lotka-Voltaire model can be represented in the following form:

$$
\begin{cases}
\dfrac{dN_1}{dt} = \left(\arg \max_{\forall Tr_j \in Tr_C^D} K_i^D \times K_i^A \right) \left(\sum_{i=1}^{Q} \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\
\qquad - \left(\sum_{i=1}^{M} \left(w_{CPSi}^C \cap w_{CPSi}^I \cap w_{CPSi}^A \cap w_{CPSi}^{Au} \cap w_{CPSi}^{Aff} \right) \chi_i^{CPS} \right) \tilde{N}_1 \left(N_2 \times \left| W_{hybrid\,C,I,A,Au,Af\,synerg} \right| \right); \\
\dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \tilde{N}_2 + \left(\dfrac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^{j} \times w_{kg}^{j} \right) \right) \tilde{N}_2 \tilde{N}_1.
\end{cases}
\tag{2.42}
$$

Thus, the proposed approach to the security model of cyber-physical systems allows, from a practical point of view, to consider cyberspace as an ecosystem, to take into account the computing capabilities of attackers and the focus of targeted cyberattacks. In addition, cyberattacks are considered taking into account their integration with social engineering methods, which allows attackers to form targeted attacks. The proposed model takes into account the possibility of manifestation of targeted attacks in the ecosystem of signs of synergy and hybridity, which significantly affects the quantitative indicators of assessing the current state of the security level.

Development of a security model for cyber-physical systems based on the «predator-prey» model, taking into account the possible competition of attackers in relation to the «prey»

One of the advantages of the Lotka-Volterra model is the ability to use the «biological» aspects of the «predator-prey» model, taking into account the possible struggle between the «predators» themselves under the conditions of a decrease in the population of «prey». From the point of view of the modern development of the world community, certain manifestations of competition are already manifesting in the environment of cyber intruders/cyber groups. This, on the one hand, can ensure an increase in the population of «preys», that is, increase the ability of the information protection system to resist threats, and/or timely prepare preventive measures to counter them. On the other hand, to reduce the number of «predators», that is, to reduce the variety of threats, which will allow to respond to them in a timely manner.

Taking into account the above assumptions, the «predator-prey» model is presented as:

$$
\begin{cases}
\dfrac{dN_1}{dt} = \left(\arg\max_{\forall Tr_j \in Tr_C^D} K_i^D \times K_i^A \right)\left(\sum_{i=1}^{Q}\left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\[3mm]
\quad - \left(\sum_{i=1}^{M}\left(w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \right)\chi_i^{CPS} \right)\tilde{N}_1\left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right); \\[4mm]
\dfrac{dN_2}{dt} = -\left(\dfrac{1}{M}\sum_{i=1}^{M}\nu_i \times p_{rj} \times r_{motiv} \right)\left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right) + \\[4mm]
\quad + \left(\dfrac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^j \times w_{kg}^j \right) \right)\left(\tilde{N}_2^1 \cap \tilde{N}_2^2 \cap \ldots \cap \tilde{N}_2^w \right)\tilde{N}_1,
\end{cases}
\tag{2.43}
$$

where the number of «predators» belongs to the set $\overline{\{\tilde{N}_2^j\}}$, $j \in 1, \ldots w$.

Thus, the proposed model for the security of cyber-physical systems takes into account the possible competition of attackers in relation to the «prey». This makes it possible to timely determine not only the direction of threats, but also the computational resources of the attackers, and their «simultaneous» impact can provide a «reduction» in the risk of cyber threats.

Development of a security model for cyber-physical systems based on the «predator-prey» model, taking into account the possibility of grouping attackers/cyber groups in order to achieve the goals of a cyberattack

The Lotka-Volterra model makes it possible to take into account not only the competitiveness of «predators», but also their unification. At the same time, as in any ecosystem, the emergent properties of «predators» can manifest themselves, which from the point of view of security can lead to a significant decrease in the resistance of the protection system of the business process loop or to its hacking and destruction of the continuity of business processes. Taking into account the above assumptions, the «predator-prey» model is presented as:

$$
\begin{cases}
\dfrac{dN_1}{dt} = \left(\arg\max_{\forall Tr_j \in Tr_C^D} K_i^D \times K_i^A \right)\left(\sum_{i=1}^{Q}\left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\[3mm]
\quad - \left(\sum_{i=1}^{M}\left(w_{CPSi}{}^C \cap w_{CPSi}{}^I \cap w_{CPSi}{}^A \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff} \right)\chi_i^{CPS} \right)\tilde{N}_1\left(\sum_{j=1}^{w}\tilde{N}_2^w \right); \\[4mm]
\dfrac{dN_2}{dt} = -\left(\dfrac{1}{M}\sum_{i=1}^{M}\nu_i \times p_{rj} \times r_{motiv} \right)\left(\sum_{j=1}^{w}\tilde{N}_2^w \right) + \left(\dfrac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^j \times w_{kg}^j \right) \right)\left(\sum_{j=1}^{w}\tilde{N}_2^w \right)\tilde{N}_1.
\end{cases}
\tag{2.44}
$$

Thus, the proposed model for the security of cyber-physical systems based on the «predator-prey» model makes it possible to take into account the possibilities of grouping intruders/cyber groups in order to achieve the goals of a cyberattack. This approach makes it possible to predict the «worst» options for the development of a cyberattack, as well as to formulate appropriate preventive measures.

2.5 DEVELOPMENT OF A SECURITY MODEL FOR CYBER-PHYSICAL SYSTEMS BASED ON THE «PREDATOR-PREY» MODEL, TAKING INTO ACCOUNT THE RELATIONSHIP BETWEEN «PREY SPECIES» AND «PREDATOR SPECIES»

In [2, 47, 51], the authors consider the m-dimensional case, which takes into account interactions in the «environment» of «predators», as well as interactions in the «environment» of «prey». Such a model is interesting, first of all, from the point of view of the interaction of «preys», which are understood as means/mechanisms of the information security system. At the same time, it is taken into account one of the principles of the formation of the information security system – the principle of sufficiency. In addition to this interaction in the «environment» of «predators», various tendencies are taken into account – from simple cooperation to confrontation. In the proposed model:

$$\tilde{N}_i = N_i \cdot f(N),$$

where $f(N) = r + \|A\| \times N$, $N_1, \ldots, N_m$ – the sizes of populations of m-different types of «predators» and «prey» that interact in one environment, N – a vector composed of these unknowns. The parameters in the vector r are responsible for the success (probability) of «fertility» (the emergence of new cyber threats, or means of protection, respectively, from species) ($r_i > 0$) or «mortality» ($r_i < 0$).

Matrix $\|A\|$ describes the relationship between «predators» or «prey» of different species, while [1, 2, 47, 51] a_{ij} describes the influence of species j on species i, a_{ji} describes the influence of species i on species j. Moreover, if both values a_{ij} and a_{ji} are positive, then the individuals benefit from the interaction, if both are negative, then they are at enmity with each other.

If $a_{ij} > 0$, $a_{ji} < 0$, then species i will be a predator, and species j will be a prey for it. The a_{ii} values describe the effect of a species on itself.

Taking into account the above assumptions, the «predator-prey» model is presented as:

$$
\begin{cases}
\dfrac{dN_1}{dt} = \left(\arg\max_{\forall Tr_j \in Tr_C^D} K_i^D \times K_i^A \right)\left(\sum_{i=1}^{Q} \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\
\quad - \left(\sum_{i=1}^{M} \left(w_{CPSi}^{\;C} \cap w_{CPSi}^{\;I} \cap w_{CPSi}^{\;A} \cap w_{CPSi}^{\;Au} \cap w_{CPSi}^{\;Aff} \right) \chi_i^{CPS} \right) \tilde{N}_1 \left(\sum_{j=1}^{w} \tilde{N}_2^w \right) - \varepsilon \tilde{N}_2^2; \\
\dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right)\left(\sum_{j=1}^{w} \tilde{N}_2^w \right) + \\
\quad + \left(\dfrac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right)\left(\sum_{j=1}^{w} \tilde{N}_2^w \right) \tilde{N}_1 - \xi \tilde{N}_2^2,
\end{cases}
\tag{2.45}
$$

where the coefficients ε, $\zeta > 0$, and describe the damage inflicted on themselves by the «prey» and «predator», respectively.

2.6 DEVELOPMENT OF A METHOD FOR ASSESSING THE SECURITY OF CYBER-PHYSICAL SYSTEMS BASED ON THE LOTKA-VOLTERRA «PREDATOR-PREY» MODEL

One of the features of cyber-physical systems is the absence of information security information in the infrastructure elements, the transmission of signals from sensors/sensors over open channels, and the provision of management and administration based on cloud technologies. This significantly reduces the possibility of forming a security loop, and leads to an increase in critical points for the implementation of cyberattacks. In such conditions, the security assessment must be carried out offline, which makes it possible to take into account the dynamics of both cyber threats, on the one hand, and the ability of means of protection to resist them.

Fig. 2.8 shows a block diagram of the proposed assessment method.

At the **first stage**. Formed and/or calculated:

– metric coefficients of threats;

– weighting factors of threat manifestation;

– determination of the implementation of each threat;

– determination of the implementation of threats to the security service;

– determination of the total threats to the composite security;

– determining the economic costs of preventing an attack.
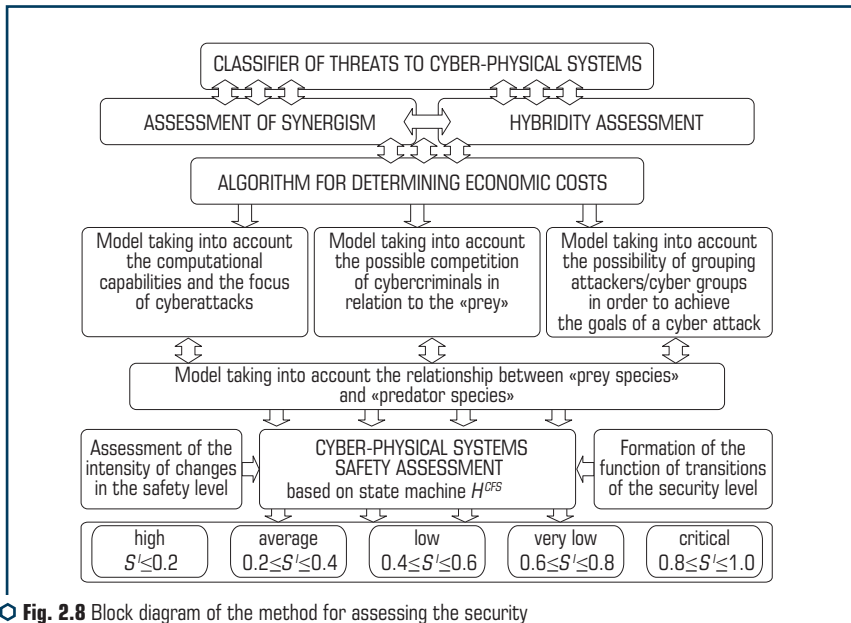
○ **Fig. 2.8** Block diagram of the method for assessing the security
of cyber-physical systems based on the Lotka-Volterra model «predator-prey»

At the **second stage**. Based on the analysis of **stage 1**, the Lotka-Volterra model is selected, and the corresponding coefficients and components of the expressions are calculated using formulas (2.29)–(2.45).

At the **third stage**, based on expressions (2.46)–(2.48), the current state of the cyberphysical system security is determined.

The proposed method is based on assessing the security of cyber-physical systems over time. A descriptive characteristic of the change in the current state of CPS safety is its *intensity* $I(t)$ – the average number of changes that have occurred with the current state of CPS safety per unit of time. To estimate the time intervals $\Delta t_{[i-q]}$ between changes, the CFS safety level, let's use the formula:

$$\Delta t_{[i-q]}(t) = \frac{K}{I(t)}, \tag{2.46}$$

where K – total number of security level changes; $I(t)$ – the intensity of changes in the level of security; $i, q \in [1;n]$ – serial numbers of changes; $i \geq q$.

Let's describe the changes in security levels in the form of an H^{CFS} state machine, the states of which are described by the formula:

$$H^{CFS} = \left\langle S^I, value, \Pi, S_0^I \right\rangle, \tag{2.47}$$

where S^I – the final state of the CFS security level; *value* – the value of changes in the CFS security level; Π – the function of transitions of the CFS security level from state k to state j; S_0^I – the initial state of the CFS security level.

Let's estimate the function of transitions of the safety level CPS Π from state k to state j by the formula:

$$\Pi = S_0^I \times value \rightarrow S^I. \tag{2.48}$$

To determine the state of safety, let's use one of the proposed Lotka-Volterra models, taking into account the possibilities of both «prey» and «predators».

The use of the proposed models for the implementation of the method for assessing the security of cyber-physical systems based on the Lotka-Volterra model is determined in **Fig. 2.9**. For modeling, the values of the parameters included in the expressions for the coefficients of the Lotka-Volterra equations are determined using the threat classifier, which already partially contains quantitative indicators. Thus, the values of the weight coefficients of the manifestation of threats are determined quantitatively. On the other hand, some of the indicators contained in the threat classifier need to be quantified.

As a conditionally real CFS, let's consider the automated banking system (ABS) of organizations in the banking sector, which not only belongs to CFS, but also to critical infrastructure systems.

To assess the security of the ABS, let's assume that the information security system has 25 technical means of information protection that provide security services to bank information resources (BIR), that is, $N_1 = 25$, the number of threats $Q = 194$ (https://bdu.fstec.ru/threat).

Their description and expert assessment of the distribution of the impact on security services are given on the resource (http://skl.hneu.edu.ua/), which makes it possible to use the proposed models to automate the calculations of the remaining indicators.
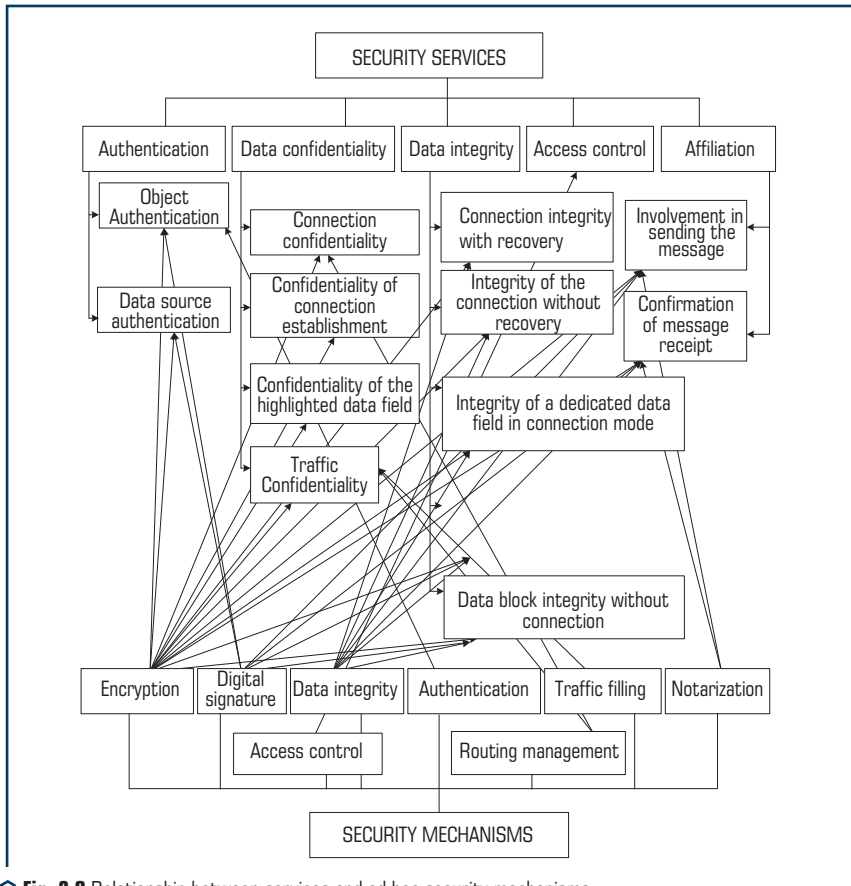
○ **Fig. 2.9** Relationship between services and ad hoc security mechanisms

Fig. 2.9 shows the relationship between security services and dedicated security mechanisms, which allows to determine the number of required technical protections (security mechanisms) to provide the corresponding security services.

The formation of a dynamic model for assessing the security of cyber-physical systems begins with the formation of metric coefficients of threats, calculated as:

$$w_j^{CPS\ CIF} = \frac{1}{K}\sum_{i=1}^{Q}\sum_{k=1}^{K} w_{ijk}^{CPS\ CIF},$$ (2.49)

where w_{CPSi}^{I}, w_{CPSi}^{I}, w_{CPSi}^{A}, w_{CPSi}^{Au}, w_{CPSi}^{Aff} are the expert weights of the security services: confidentiality, integrity, availability, authenticity, and affiliation, as previously stated.

It is proposed for experts in [2, 50] to use values:

$$w_j^{CPS\ CIF} \in \{0;\ 0.1;\ 0.25;\ 0.33;\ 0.5;\ 0.66;\ 0.75;\ 0.9;\ 1\}$$

to form the weighting factors of the cyber threat impact on security services. 27 experts took part in the formation of an expert assessment.

Then, based on the averaged values of the weight coefficients for the security service, let's determine the distribution of technical means of information security as:

$$\lambda_j^{CPS\ CIF} = N_1^j \times w_j^{CPS\ CIF},$$ (2.50)

where j – a security service; N_1^j – the number of «prey» objects (technical means of information security). A limitation in modeling is the assumption that the technical means of information security cannot provide several security services.

Table 2.4 shows the results of distribution by experts of the weights of the main services: confidentiality, integrity, availability and authenticity, as well as the average values of the weights of the distribution of technical means of protection for security services.

To determine the cost indicators of attacks, let's use the table of the size of possible losses of the FAIR (Factor Analysis of Information Risk) risk assessment methodology [28, 29].

Let's estimate the costs of attackers for carrying out attacks on the assumption that they amount to no more than 10 % of the amount of possible losses of the prey (**Table 2.5**).

Then the coefficients of the model are calculated in accordance with the previously derived relationships.

Fertility rate of «preys» in accordance with the proposals on the available resources of «preys» and «predators» (**Table 2.4**) and the total number of threats:

$$\alpha = \frac{\left|\{Tr_j\}\right|}{Q} = \frac{29}{194} = 0.15.$$ (2.51)

To calculate the coefficient of the influence of the predator on the prey (β), let's assume that the number of «predators» (intruders and/or groups of cyber intruders) is $N_2 = 5$, and

$\left|W_{hybrid\,C,I,A,Au,Af\,synerg}\right| = 0.03$, at the same time the weighting coefficient of the influence of each threat let's choose the maximum 0.33, i.e. each of the 194 threats is implemented by cyber-criminals every day. The coefficient β of the impact of modern threats on protective equipment, presented earlier as:

$$\beta = \sum_{i=1}^{M}\left(w_{CPSi}{}^{C} \cap w_{CPSi}{}^{I} \cap w_{CPSi}{}^{A} \cap w_{CPSi}{}^{Au} \cap w_{CPSi}{}^{Aff}\right)\chi_i^{CPS},$$

largely depends on expert assessments. Based on the opinion of experts, let's get the value of the coefficient $\beta = 0.32$.

● **Table 2.4** The results of an expert assessment of the weights of the impact of cyber threats on security services

No. threat, i	Weights for the Impact of Cyber Threats on Security Services				
	A_i^C	A_i^{Au}	A_i^A	A_i^I	A_i^{Aff}
1	0.28	0.22	0.2	0.21	0.09
2	0.19	0.22	0.23	0.23	0.13
3	0.22	0.15	0.25	0.28	0.1
4	0.21	0.19	0.13	0.3	0.17
5	0.15	0.2	0.36	0.22	0.07
…	…	…	…	…	…
190	0.24	0.21	0.15	0.4	0
191	0.15	0.19	0.15	0.5	0.01
192	0.35	0.17	0.12	0.36	0
194	0.32	0.31	0.12	0.18	0.07
averaged values of the weighting factors for the security service					
$w_j^{CPS\,CIF}$	$w_{CPSi}{}^{C}$	$w_{CPSi}{}^{Au}$	$w_{CPSi}{}^{A}$	$w_{CPSi}{}^{I}$	$w_{CPSi}{}^{Aff}$
	0.26	0.22	0.26	0.25	0.01

● **Table 2.5** Potential Loss Rate (PLM) (USD)

No.	losses	lower limit	upper limit
1	Critical	10 000 000	–
2	High	1 000 000	9 999 999
3	Significant	100 000	999 999
4	Average	10 000	99 999
5	Low	1 000	9 999
6	Very Low	0	999

To calculate the mortality rate of a predator (φ), let's use the data from **Table 2.5**, and also believe that $M = \left|\left\{Tr_i\right\}\right|$. Based on the estimates given in [1, 2, 7, 47, 51], as well as expert estimates, let's obtain the numerical value of the coefficient φ, which determines the rate of mortality of «predators» in the Lotka-Volterra model $\varphi = 0.29$.

To calculate the coefficient of the prey's influence on the predator (γ), let's use the indicator $B = 3$ – security services, where cryptographic means of protection (confidentiality, integrity, authenticity) are used. In this case, let's assume that the set of characteristics of cryptographic means of protecting the security information system $\mu^j = \left|\left\{C_r^j, S_c^j, O_E^j\right\}\right|$, the weight coefficients for symmetric systems are equal to 0.75, for asymmetric cryptosystems 0.9. The final value of the coefficient γ, which determines the influence of the «prey» on the «predator», is 0.27.

The initial values of «prey» and «predator» are equal, respectively.

$$\tilde{N}_1 = 55 \times 0.26 + 49 \times 0.22 + 73 \times 0.26 + 17 \times 0.25 \approx 48,$$

$$\tilde{N}_2 = N_2 \times \left|W_{hybrid\ C,I,A,Au,Af\ synerg}\right| = 5 \times 9 = 45.$$

The number of hybrid threats is determined in accordance with the threat classifier.

The performed calculations allow to obtain the numerical values of the coefficients included in the Lotka-Volterra equations.

Parameterized equations allow modeling the dynamics of the development of a cyber-physical system in the context of the manifestation of hybridity and synergy of threats. The results of modeling the behavior of a conditionally real system are shown in **Fig. 2.10–2.16**.

Fig. 2.10 shows the dynamics of changes in the number of potential targets and threats.
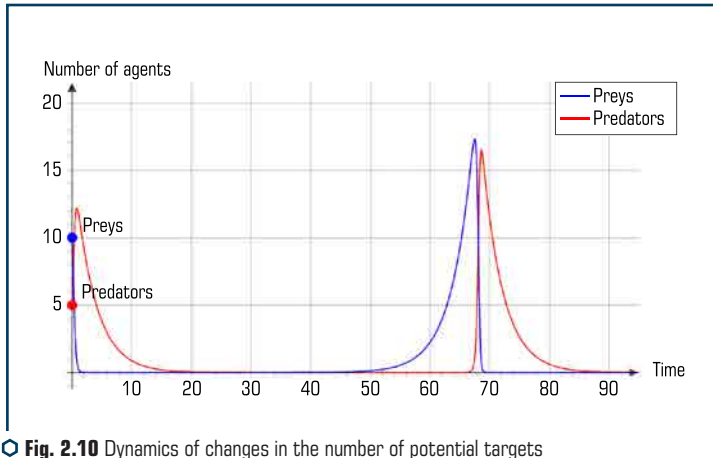
○ **Fig. 2.10** Dynamics of changes in the number of potential targets and threats, with $\alpha = 0.29$, $\beta = 0.32$, $\gamma = 0.29$, $\varphi = 0.29$

With an increase in the number of critical attacks, the interaction between prey and predators becomes more intense, i.e. the period between growth and decline in the number of both sides of the cyber conflict is shrinking (**Fig. 2.11**).

A more visual representation of the simulation results can be obtained by presenting the results in the form of a phase portrait. A phase portrait (aka phase diagrams) is a graphical representation of how the quantities describing the state of the system (dynamic variables) depend on each other. In our case, this is the number of predators and prey. A typical phase portrait for dynamic variables of the Lotka-Volterra model is shown in **Fig. 2.12** (the coefficients of the model correspond to the calculated ones of the considered problem).
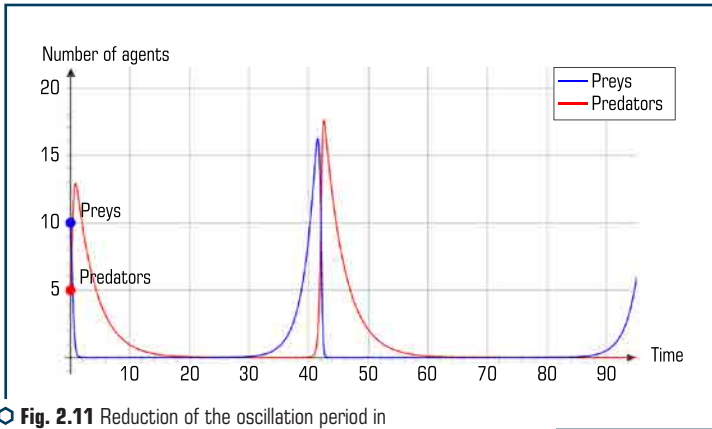
○ **Fig. 2.11** Reduction of the oscillation period in
the «predator-prey» system, $\alpha=0.49$, $\beta=0.32$, $\gamma=0.29$, $\varphi=0.29$
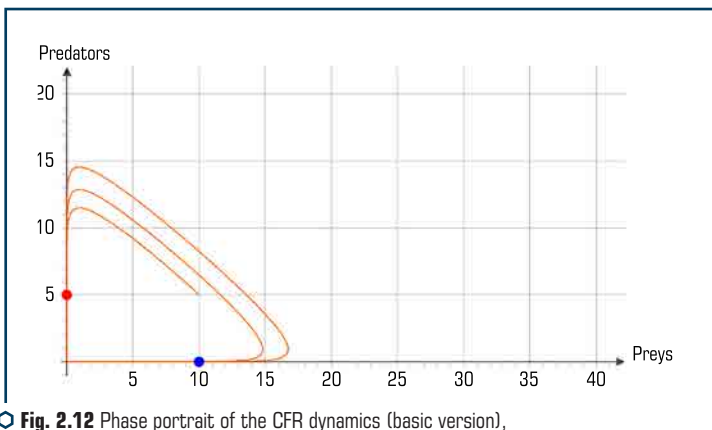
○ **Fig. 2.12** Phase portrait of the CFR dynamics (basic version),
with $\alpha=0.28$, $\beta=0.33$, $\gamma=0.29$, $\varphi=0.28$

With an increase in the number of critical threats, the total number of threats also increases, and therefore the coefficient α also changes. For the new values of the number of critical threats and the birth rate of «preys», the phase portrait will have the form shown in **Fig. 2.13**.

○ **Fig. 2.13** Phase portrait with a change in the birth rate of preys, with $\alpha=0.39$, $\beta=0.32$, $\gamma=0.29$, $\varphi=0.27$
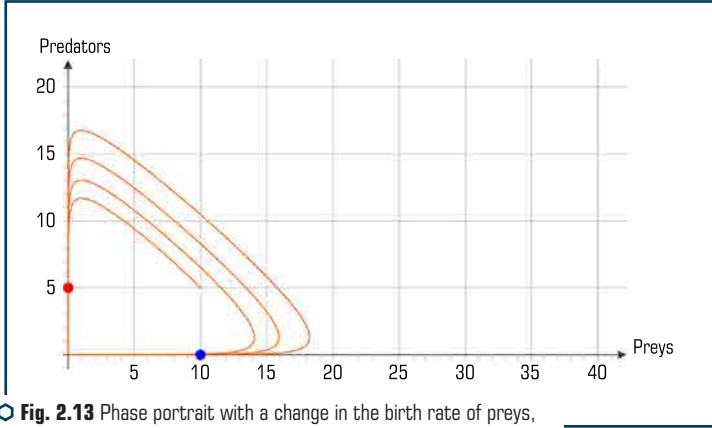
With an increase in the coefficient β, i.e. more intense influence of predators on prey even with an increase in the number of potential targets (prey), the number of predators not only does not grow, but also decreases. This can be explained by the fact that with a more intense impact, the same amount of compromised resources can be reached by a smaller number of predators (**Fig. 2.14**).

○ **Fig. 2.14** Phase portrait of the system with an increase in the influence of predators on prey (more aggressive conduct of cyberattacks), with $\alpha=0.25$, $\beta=0.76$, $\gamma=0.29$, $\varphi=0.27$
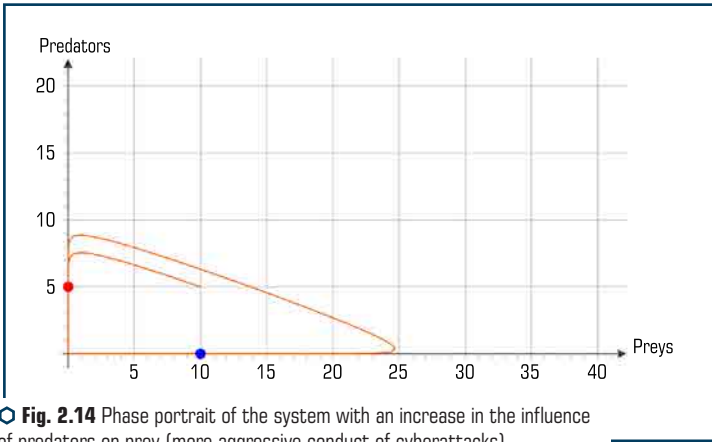
An increase in the mortality rate of predators, as shown by simulation experiments, insignificantly affects the increase in the number of prey, but leads to more intensive attacks by predators (**Fig. 2.15**).

With an increase in the coefficient of the prey's influence on the predator, the phase portrait has the form shown in **Fig. 2.16**. The results obtained can be interpreted as the need to increase the number of predators in order to achieve targets with the same or even less prey.
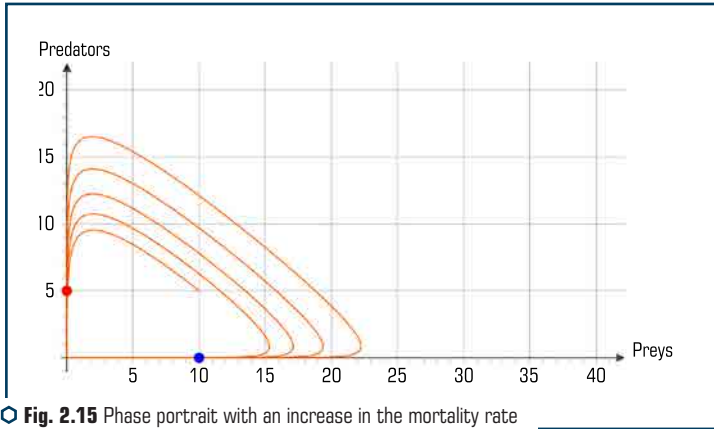
○ **Fig. 2.15** Phase portrait with an increase in the mortality rate of predators, with $\alpha=0.25$, $\beta=0.32$, $\gamma=0.58$, $\varphi=0.27$
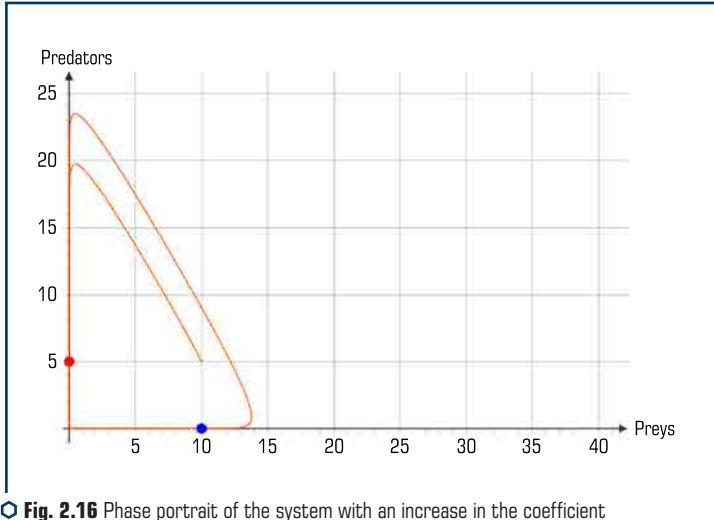
○ **Fig. 2.16** Phase portrait of the system with an increase in the coefficient of the prey's influence on the predator, with $\alpha=0.25$, $\beta=0.32$, $\gamma=0.29$, $\varphi=0.54$

Analysis of the simulation results (**Fig. 2.10–2.16**) allows to make a fairly general conclusion that in the context of limited financial resources allocated for the development and implementation of new tools that provide security services, their distribution should be carried out as follows. One of the coefficients is determined, the change of which leads to more significant changes in terms of the level of safety. The most significant factor that leads to changes in the considered coefficient is found out. The activities that lead to such changes are determined. **Table 2.6** shows the comparative results of the analysis of the practical use of the method for assessing the state of security of cyber-physical systems based on the Lotka-Voltera model.

● **Table 2.6** Results of the study of the practical use of the method for assessing the state of security of cyber-physical systems based on the Lotka-Voltera model

Methods	Criteria								
	qualitative assessment	quantitative assessment	comprehensive assessment	assessment of threat characteristics		economic optimization	assessment of compliance with regulatory standards	effectiveness of preventive measures	evaluation mode
				hybridity	synergy				
NIST	+	–	–	–	–	–	–	–	stat.
FAIR	–	–	+	–	–	–	–	+	stat.
EBIOS	+	–	–	–	–	–	–	+	stat.
MEHARI	–	–	+	–	–	–	–	–	stat.
OCTAVE	+	–	–	–	–	–	–	–	stat.
IT-GRUND-SHULTZ	+	–	–	–	–	–	–	+	stat.
IRAM	+	–	–	–	–	–	–	–	stat.
RISK WATCH	–	+	–	–	–	–	–	+	stat.
FRAP	+	–	–	–	–	–	–	–	stat.
CRAMM	–	–	+	–	–	–	–	+/–	stat.
MAGERIT	+	+	–	–	–	–	–	–	stat.
Method in [13]	+	+	–	–	–	–	–	+/–	dynamic
Method in [23]	+	+	–	–	–	–	–	+/–	dynamic
Suggested method	+	+	+	+	+	+	+	+/–	dynamic

Analysis of the **Table 2.6** shows that almost all practical approaches to safety assessment operate in a static mode, that is, during working hours, incident detection systems (deviations

from normal operation) record incidents/threats, and their analysis is carried out outside of working hours. This approach does not allow timely consideration of the synergy and hybridity of targeted attacks, the need for preventive measures. The proposed method and the methods in [2, 47] use approaches to assessing security based on the Lotka-Voltaire model, which makes it possible to conduct an assessment in a dynamic mode (in real time to assess the dynamics of threats, their capabilities). However, the works [2, 47] do not take into account the synergy and hybridity of modern threats, their possibility of being integrated with the methods of social engineering. In the proposed method, on the basis of the proposed classifier, these signs of threats are taken into account, which makes it possible to obtain the coefficients of the model and, knowing the number of threats, to determine the number of threats with these signs.

So, in the example under consideration, with the total number of threats $Q = 194$, the coefficient of the influence of the predator on the prey (the coefficient of predation) makes it possible to determine the number of threats with signs of synergy and hybridity (with $\beta = 0.32$, the number of threats $Q_{synerg} = Q \times \beta = 194 \times 0.32 = 62.08$). In addition, it, in turn, depends on the introduction of new means of ensuring security services; as an investment, it makes sense to choose those protection means (confidentiality, integrity, authenticity), the weight of which has the maximum value. As mentioned earlier, the weighting factor for asymmetric cryptographic protections is 0.9, as opposed to symmetric (0.75). It is on the development of these means of protection that the available resources should be directed in the first place.

2.7 DEVELOPMENT OF SOCIO-CYBER-PHYSICAL SYSTEMS SECURITY CONCEPT

The development of industry 4.0 forms the superstructure of the synthesis of social networks with cloud technologies and various classical networks of global and local systems. Integration is based on interconnection between rapidly developing technologies of mobile technologies based on wireless Internet standards – LTE technologies (Long-Term Evolution), IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth [1–4]. In the context of the formation of a high-tech society, social networks based on Internet services have become one of the most effective and popular means of mass communication. Influencing such communities is an effective mechanism of influence in the context of hybrid wars and color revolutions [1, 2, 47, 52–58]. Such a synthesis of social Internet services (SIS) with cyber-physical systems makes it possible to form a socio-cyber-physical system (cyberphysical social system, CPSS) [52–56]. CPSS allows to form the social, political, economic «opinion» of the intellectual community (integration of the cybernetic, physical and social worlds), regulate and manage based on the SIS, provide users with proactive services. The nature of CPSS data brings new requirements and challenges to the various stages of data processing, including the identification of data sources, the processing and aggregation of data of various types and scales.

On the one hand, this approach allows to significantly speed up the process of introducing smart technologies, expand the range of services and switch to mesh and NGN network technologies,

on the one hand. On the other hand, it creates the need to ensure security in various technology planes. In addition, the development of quantum algorithms by Grover and Shor calls into question the stability of systems of symmetric and asymmetric cryptography, which can lead to «chaos» in security, and the need to form fundamentally new approaches to assessing threats, creating security loops for business processes (internal and external) taking into account the integration and globalization of WAN network technologies, cloud technologies based on wireless channel standards IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth, LTE [1, 2, 47, 52–58].

Fig. 2.17 presents a structural and logical diagram of socio-cyber-physical systems, which allows to consider the integration of social and cyberspace as a combination of the use of individual components technologies of such platforms as social, cyberspace and cyber-physical networks. This approach takes into account not only the logical component of the individual elements functionality of the socio-cyber-physical systems infrastructure, but also creates the need to integrate and develop a new concept of a multi-level/multi-loop security system, taking into account modern vectors of cyberattacks.
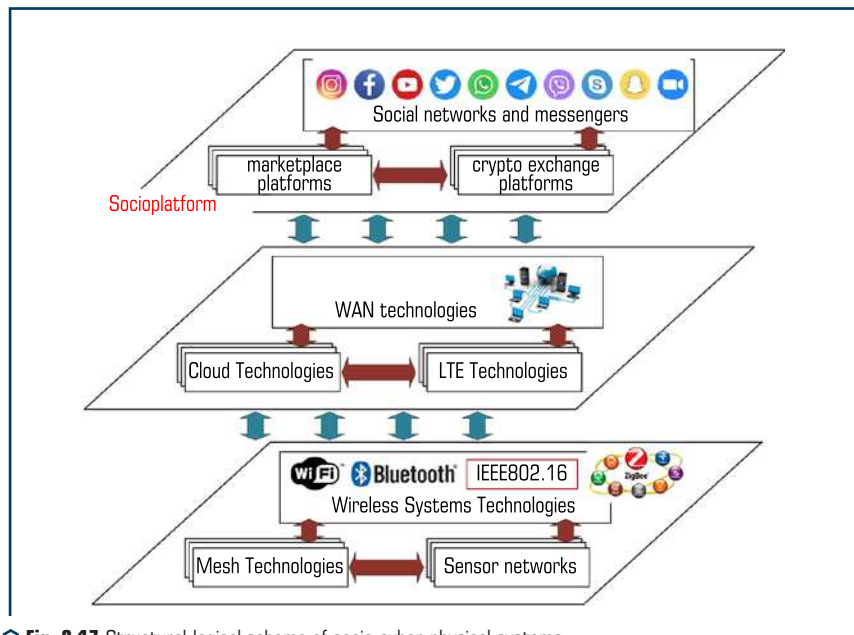
○ **Fig. 2.17** Structural-logical scheme of socio-cyber-physical systems

The formation of socio-cyber-physical systems allows to consider the integration of the functionality of social networks into cyberspace – the combination of global computer networks with mobile and cloud technologies, the integration of classical networks with smart technologies make

it possible to form a transition to NGN networks and significantly integrate one technology into another (**Fig. 2.17**). To ensure the formation of the concept, **Fig. 2.18** shows a block diagram of the main technologies that allow the formation of socio-cyber-physical systems.
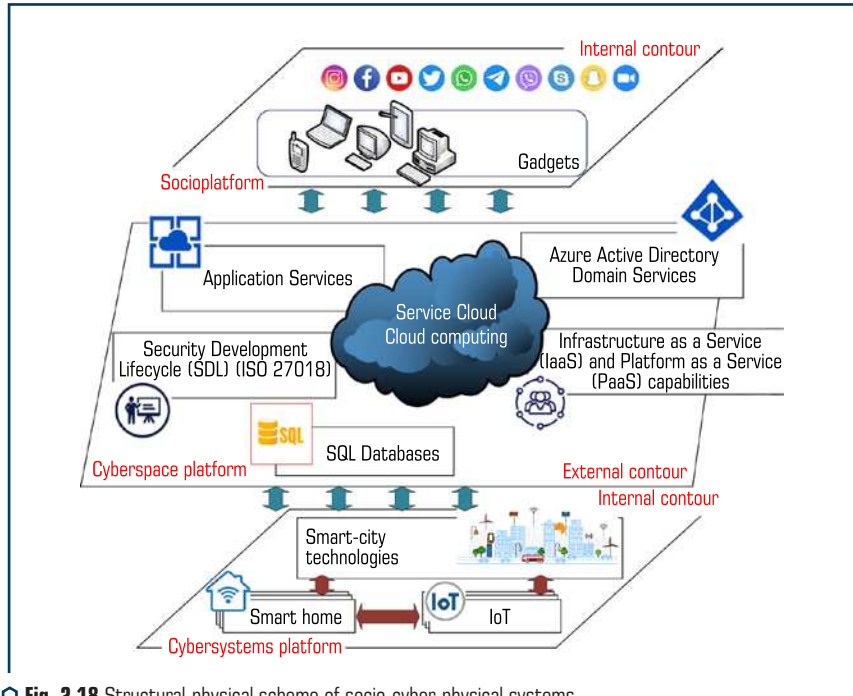
○ **Fig. 2.18** Structural-physical scheme of socio-cyber-physical systems

A variety of devices that can be used in complex information and communication systems (information and communication systems, ICS) and cyber-physical systems (cyberphysical systems, CPS) make it possible to form the concept of a socio-cyber-physical system (CPSS) with SIS. CPSS is a set of subjects and objects of the cybernetic, physical and social worlds that allow the formation of «smart» communities, on the one hand, and intellectual space, on the other. In CPSS, users are service consumers, and physical objects in the form of various devices are service providers.

Thus, the formation of socio-cyber-physical systems can be considered as the integration of various cyber-physical systems and mobile Internet technologies [1, 2, 47, 59–61]. To ensure security in cyber-physical systems and smart technologies, the KNX standard (ISO/IEC 14543) is usually used, which provides security services – data confidentiality and integrity [47, 59–61]. However, the formation of security is considered only at the level of the cyber-physical system separately, and the control system, which is deployed on the basis of cloud technologies, is not

taken into account. So, the security system provides only security services within the loop of the cyber-physical system, and intruders have the ability to use control commands both to and from the cloud. In addition, a significant security problem for cyber-physical systems is the use of wireless/mobile data transmission channels between sensors and the switching system of cyber-physical systems, as well as the integration of «additional hacking elements» into the network infrastructure – the Internet of Things. To ensure security in the post-quantum period (the advent of a full-scale quantum computer), the paper [61] proposes the concept of security of cyber-physical systems based on two security loops (the internal one is the physical mesh/sensor network itself, and the outer loops is the control system that is deployed on the basis of cloud technologies). However, this approach does not take into account the integration of technologies and does not consider the integration of the three main components of the power of the networks themselves. The proposed Security Concept for socio-cyber-physical systems not only takes into account the logical and physical structures of the CPSS, but also ensures the interaction between the power of certain networks and the technologies that are used to form them. **Fig. 2.19** shows a block diagram of the Concept of multi-loop security of socio-cyber-physical systems.
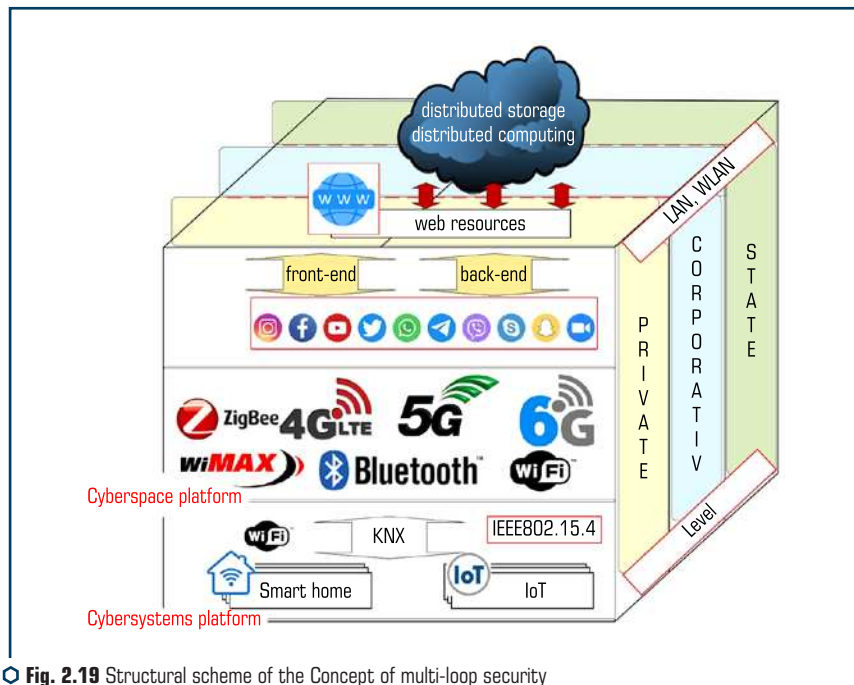
○ **Fig. 2.19** Structural scheme of the Concept of multi-loop security of socio-cyber-physical systems

One of the aspects of this Concept is taking into account the interconnections of various cyber-physical systems, taking into account property rights, as well as the synergy and hybridity of modern targeted attacks, based on the integration of cyber threats with social engineering methods.

Fig. 2.20 shows the relationship of such systems, taking into account their forms of ownership and targeted threats.
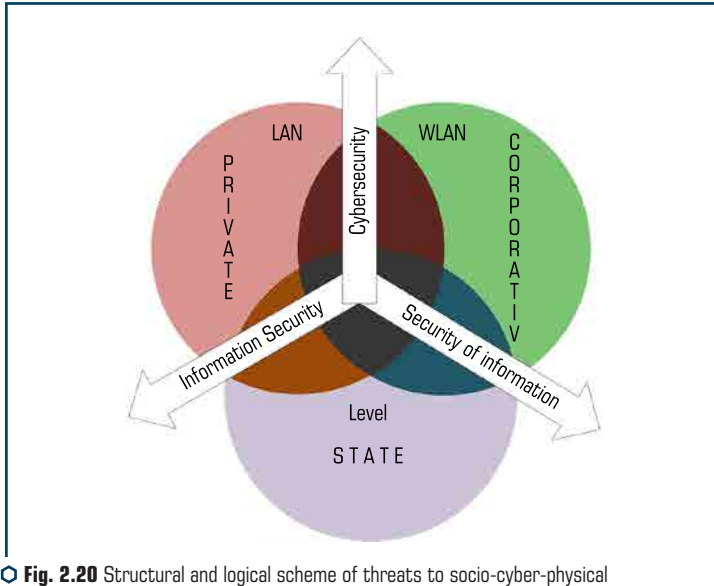
○ **Fig. 2.20** Structural and logical scheme of threats to socio-cyber-physical systems, taking into account the form of power

For a formal description of the Concept, let's use the approach in [61]: to ensure the security of the entire protection system, it is necessary to take into account the threats of the internal and external loops for each of the platforms:

– *threats of the internal loop, taking into account the hybridity and synergy of threats* for the 1st platform – social networks:

$$W^{SS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{1platform}} =$$

$$= W^{SS\ ISL}_{synerg_{1platform}}{}^{C} \bigcap W^{SS\ ISL}_{synerg_{1platform}}{}^{I} \bigcap W^{SS\ ISL}_{synerg_{1platform}}{}^{A} \bigcap W^{SS\ ISL}_{synerg_{1platform}}{}^{Au} \bigcap W^{SS\ ISL}_{synerg_{1platform}}{}^{Inv}, \qquad (2.52)$$

where $W^{SS\ ISL}_{synerg_{1platform}}{}^{C}$ – synergy of threats to the confidentiality service; $W^{SS\ ISL}_{synerg_{1platform}}{}^{I}$ – synergy of threats to the integrity service; $W^{SS\ ISL}_{synerg_{1platform}}{}^{A}$ – synergy of threats to the availability service;

$W_{synerg_{1platform}}^{SS\,ISL\quad Au}$ — synergy of threats to the authenticity service; $W_{synerg_{1platform}}^{SS\,ISL\quad Inv}$ — synergy of threats to the involvement service.

— *threats of the internal loop, taking into account the hybridity and synergy of threats* for the 2nd platform — cyberspace:

$$W_{hybrid\,C,I,A,Au,Af\,synerg_{2platform}}^{CS\,ISL} =$$

$$= W_{synerg_{2platform}}^{CS\,ISL\quad C} \bigcap W_{synerg_{2platform}}^{CS\,ISL\quad I} \bigcap W_{synerg_{2platform}}^{CS\,ISL\quad A} \bigcap W_{synerg_{2platform}}^{CS\,ISL\quad Au} \bigcap W_{synerg_{2platform}}^{CS\,ISL\quad Inv}, \quad (2.53)$$

where $W_{synerg_{2platform}}^{CS\,ISL\quad C}$ — synergy of threats to the confidentiality service; $W_{synerg_{2platform}}^{CS\,ISL\quad I}$ — synergy of threats to the integrity service; $W_{synerg_{2platform}}^{CS\,ISL\quad A}$ — synergy of threats to the availability service; $W_{synerg_{2platform}}^{CS\,ISL\quad Au}$ — synergy of threats to the authenticity service; $W_{synerg_{2platform}}^{CS\,ISL\quad Inv}$ — synergy of threats to the involvement service.

— *threats of the internal loop, taking into account the hybridity and synergy of threats* for the 3rd platform — cyber-physical systems:

$$W_{hybrid\,C,I,A,Au,Af\,synerg_{3platform}}^{CPS\,ISL} =$$

$$= W_{synerg_{3platform}}^{CPS\,ISL\quad C} \bigcap W_{synerg_{3platform}}^{CPS\,ISL\quad I} \bigcap W_{synerg_{3platform}}^{CPS\,ISL\quad A} \bigcap W_{synerg_{3platform}}^{CPS\,ISL\quad Au} \bigcap W_{synerg_{3platform}}^{CPS\,ISL\quad Inv}, \quad (2.54)$$

where $W_{synerg_{3platform}}^{CPS\,ISL\quad C}$ — synergy of threats to the confidentiality service; $W_{synerg_{3platform}}^{CPS\,ISL\quad I}$ — synergy of threats to the integrity service; $W_{synerg_{3platform}}^{CS\,ISL\quad A}$ — synergy of threats to the availability service; $W_{synerg_{3platform}}^{CS\,ISL\quad Au}$ — synergy of threats to the authenticity service; $W_{synerg_{2platform}}^{CS\,ISL\quad Inv}$ — synergy of threats to the involvement service.

General assessment of threats of the internal loop, taking into account the technologies of the socio-cyber-physical system:

$$W_{ISL}^{CPSS} = W_{hybrid\,C,I,A,Au,Af\,synerg_{1platform}}^{SS\,ISL} \bigcup W_{hybrid\,C,I,A,Au,Af\,synerg_{2platform}}^{CS\,ISL} \bigcup W_{hybrid\,C,I,A,Au,Af\,synerg_{3platform}}^{CPS\,ISL}. \quad (2.55)$$

General assessment of threats of the internal loop, taking into account the form of ownership of the elements and technologies of the socio-cyber-physical system (**Fig. 2.20**):

$$W_{ISL_{general}}^{CPSS} = W_{ISL_{private.}}^{CPSS} \bigcup W_{ISL_{state}}^{CPSS} \bigcup W_{ISL_{corporativ}}^{CPSS}, \quad (2.56)$$

where $W_{ISL_{private.}}^{CPSS}$ — overall assessment of internal loop threats to the personal property system; $W_{ISL_{state}}^{CPSS}$ — overall assessment of threats of the internal loop for the state property system; $W_{ISL_{corporativ}}^{CPSS}$ — overall assessment of threats of the internal loop for the corporate property system;

— *threats of the external loop, taking into account hybridity and synergy of threats* for the 1st platform — social networks:

$$W_{\text{hybrid } C,I,A,Au,Af\, synerg_{1platform}}^{SS\,ESL} =$$

$$= W_{synerg_{1platform}}^{SS\,ESL\quad C} \bigcap W_{synerg_{1platform}}^{SS\,ESL\quad I} \bigcap W_{synerg_{1platform}}^{SS\,ESL\quad A} \bigcap W_{synerg_{1platform}}^{SS\,ESL\quad Au} \bigcap W_{synerg_{1platform\,\partial}}^{SCPS\,ESL\quad Inv}, \qquad (2.57)$$

where $W_{synerg_{1platform}}^{SS\,ESL\quad C}$ — synergy of threats to the confidentiality service; $W_{synerg_{1platform}}^{SS\,ESL\quad I}$ — synergy of threats to the integrity service; $W_{synerg_{1platform}}^{SS\,ESL\quad A}$ — synergy of threats to the availability service; $W_{synerg_{1platform}}^{SS\,ESL\quad Au}$ — synergy of threats to the authenticity service; $W_{synerg_{1platform}}^{SS\,ESL\quad Inv}$ — synergy of threats to the involvement service.

– *threats of the external loop, taking into account hybridity and synergy of threats* for the 2nd platform – cyberspace:

$$W_{\text{hybrid } C,I,A,Au,Af\, synerg_{2platform}}^{CS\,ESL} =$$

$$= W_{synerg_{2platform}}^{CS\,ESL\quad C} \bigcap W_{synerg_{2platform}}^{CS\,ESL\quad I} \bigcap W_{synerg_{2platform}}^{CS\,ESL\quad A} \bigcap W_{synerg_{2platform}}^{CS\,ESL\quad Au} \bigcap W_{synerg_{2platform}}^{CS\,ESL\quad Inv}, \qquad (2.58)$$

where $W_{synerg_{2platform}}^{CS\,ESL\quad C}$ — synergy of threats to the confidentiality service; $W_{synerg_{2platform}}^{CS\,ESL\quad I}$ — synergy of threats to the integrity service; $W_{synerg_{2platform}}^{CS\,ESL\quad A}$ — synergy of threats to the availability service; $W_{synerg_{2platform}}^{CS\,ESL\quad Au}$ — synergy of threats to the authenticity service; $W_{synerg_{2platform}}^{CS\,ESL\quad Inv}$ — synergy of threats to the involvement service.

– *threats of the external loop, taking into account hybridity and synergy of threats* for the 3rd platform – cyber-physical systems:

$$W_{\text{hybrid } C,I,A,Au,Af\, synerg_{3platform}}^{CPS\,ESL} =$$

$$= W_{synerg_{3platform}}^{CPS\,ESL\quad C} \bigcap W_{synerg_{3platform}}^{CPS\,ESL\quad I} \bigcap W_{synerg_{3platform}}^{CPS\,ESL\quad A} \bigcap W_{synerg_{3platform}}^{CPS\,ESL\quad Au} \bigcap W_{synerg_{3platform}}^{CPS\,ESL\quad Inv}, \qquad (2.59)$$

where $W_{synerg_{3platform}}^{CPS\,ESL\quad C}$ — synergy of threats to the confidentiality service; $W_{synerg_{3platform}}^{CPS\,ESL\quad I}$ — synergy of threats to the integrity service; $W_{synerg_{3platform}}^{CS\,ESL\quad A}$ — synergy of threats to the availability service; $W_{synerg_{3platform}}^{CS\,ESL\quad Au}$ — synergy of threats to the authenticity service; $W_{synerg_{3platform}}^{CS\,ESL\quad Inv}$ — synergy of threats to the involvement service.

General assessment of threats of the internal loop, taking into account the technologies of the socio-cyber-physical system:

$$W_{ESL}^{CPSS} = W_{\text{hybrid } C,I,A,Au,Af\, synerg_{1platform}}^{SS\,ESL} \bigcup W_{\text{hybrid } C,I,A,Au,Af\, synerg_{2platform}}^{CS\,ESL} \bigcup W_{\text{hybrid } C,I,A,Au,Af\, synerg_{3platform}}^{CPS\,ESL}. \qquad (2.60)$$

General assessment of threats of the internal loop, taking into account the form of ownership of the elements and technologies of the socio-cyber-physical system (**Fig. 2.20**):

$$W_{ESL_{general}}^{CPSS} = W_{ESL_{private.}}^{CPSS} \bigcup W_{ESL_{state}}^{CPSS} \bigcup W_{ESL_{corporativ}}^{CPSS},$$ (2.61)

where $W_{ESL_{private.}}^{CPSS}$ – overall assessment of internal loop threats to the personal property system; $W_{ESL_{state}}^{CPSS}$ – overall assessment of threats of the internal loop for the state property system; $W_{ESL_{corporativ}}^{CPSS}$ – overall assessment of threats of the internal loop for the corporate property system.

Based on expressions (2.52), (2.60), an assessment of threats in socio-cyber-physical systems in the internal and external security loops of the CPSS is formed, and on the basis of expressions (2.53), (2.61) – taking into account the forms of ownership (separately). To provide a generalized assessment of a multiloop security system, let's use the formula:

$$W_{final}^{CPSS} = W_{ISL_{general}}^{CPSS} \bigcup W_{ESL_{general}}^{CPSS}.$$ (2.62)

Each element of information resources $I_{A_i} \in \{I_A\}$ can be described by a vector:

$$I_{A_i} = \left(Type_i, A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}, \beta_i\right).$$

$Type_i$ – information asset type, described by a set of basic values: $Type_i = \{CI_i,\ PD_i,\ CD_i,\ TS_i,\ StR_i,\ Publ_i,\ Contl_i,\ PI_i\}$, where CI_i – confidential information, PD_i – payment documents, CD_i – loan documents, TS_i – commercial secret, StR_i – statistical reports, $Publ_i$ – public information, $Contl_i$ – control information, PI_i – personal data; $A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}$ – security services (A_i^C – confidentiality, A_i^I – integrity, A_i^A – availability, A_i^{Au} – authenticity, A_i^{Inv} – involvement); β_i – a metric of the ratio of time and information confidentiality degree for an asset (critical – 1.0; high – 0.75; medium – 0.5; low – 0.25; very low – 0.01).

Then the general (current) level of socio-cyber-physical systems security based on wireless mobile technologies is described by the expression:

– for additive convolution:

$$L_{W_{security}^{CPSS}} = L_{ISL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij}\right) + L_{ESL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij}\right);$$ (2.63)

– for multiplicative convolution:

$$L_{W_{security}^{CPSS}} = 1 - \left[1 - L_{ISL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij}\right)\right] \times \left[1 - L_{ESL} \sum_{j=1}^{3} \sum_{i=1}^{12} \left(I_{A_{ij}} \times \beta_{ij}\right)\right].$$ (2.64)

Thus, this approach provides an objective assessment of cyber threats to socio-cyber-physical systems, taking into account their hybridity and synergy, as well as possible integration and globalization of technologies and forms of ownership.

2.8 DEVELOPMENT OF A METHOD FOR ASSESSING FORECAST OF SOCIAL IMPACT IN REGIONAL COMMUNITIES

Achievements in the field of information technology were a prerequisite for the creation of a new form of social groups, called «virtual communities», the influence on which can allow achieving the necessary target states or the reactions of such communities. The virtual community is a reflection of the connections, relationships and interactions of people taking place in social life, but every day they are more and more regularly transferred to free and boundless cyberspace.

The identification of such communities and groups in the network and the identification of the most influential agents will determine the degree and direction of the necessary social influences to achieve the goals set.

The integration of CPSS with «virtual communities» greatly influences the tasks of forming both political, social and economic worldviews. The latter can be formed on the basis of the influence of both state subjects of government, political parties, and informal leaders of the regional community. The block diagram of the CPSS is shown in **Fig. 2.21**.
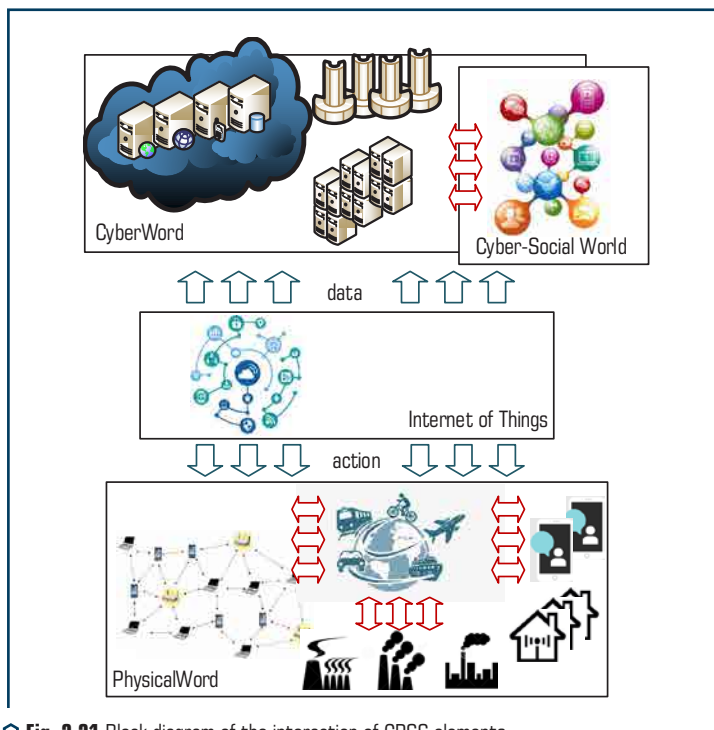
○ **Fig. 2.21** Block diagram of the interaction of CPSS elements

A variety of devices that can be used in integrated information and communication systems (ICS) and cyberphysical systems (CPS) make it possible to form the concept of a socio-cyberphysical system (CPSS) with the SIS. CPSS is a set of subjects and objects of the cybernetic, physical and social worlds, which make it possible to form «smart» communities, on the one hand, and intellectual space, on the other. In CPSS, users are service consumers, and physical entities in the form of various devices are service providers [2, 47].

Thus, the integration of the cybernetic, physical and social worlds allows the creation of smart communities, that is, those capable of behaving rationally. From a social point of view, smart communities can promote social awareness among members using certain social sensors [2, 47].

To study the features of the creation and development of virtual (smart) communities, specialized research organizations have been created. Among them are such as «Communication Institute for Online Scholarship», «The UCLA Center for the Study of Online Community», «Association of Internet Researchers», «International Society for Mental Health Online», «The Society for Computers in Psychology» [62]. The results of the work of such organizations are of particular importance for structures seeking to establish their presence in the electronic environment, as well as for scientists trying to understand the behavior of Internet users. However, despite the fact that such studies have been carried out for quite a long time, at the moment the mechanisms and methods of purposeful influence on social communities have not been sufficiently developed, which makes it possible to judge the prospects of the stated research topic.

Thus, CPSS allow not only to form and develop the functions of a smart community and intellectual space, but also to influence the behavior of communities through the SIS, ensuring the formation of a predictable worldview. Assessment of the impact on social groups in the regional community in this aspect affects the national security of the state as a whole, which confirms the relevance of this area of research. One of the main points in determining the impact on a community and a social group is the very selection of this community within the entire social network or society as a whole.

A community is defined as a group of nodes with tighter internal connections than with the rest of the network [63]. This intuitive definition has been formalized in several competing ways, usually as a quality function that quantifies the quality of a given division of the network into communities. The main approaches to isolating a community from a network are shown in **Fig. 2.22**.
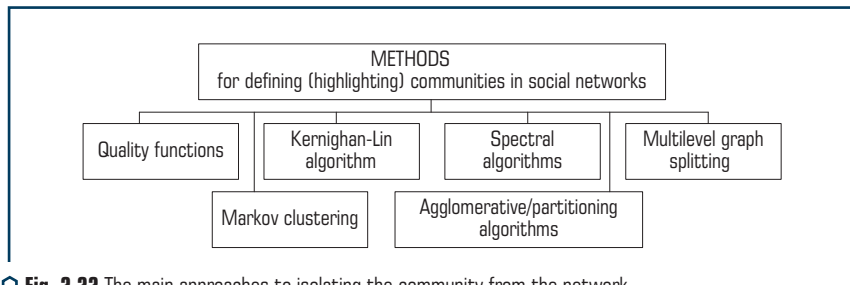
○ **Fig. 2.22** The main approaches to isolating the community from the network

The features of each of the methods are discussed below.

Quality functions. In the literature [63, 64], many functions or quality indicators have been proposed to reflect the quality of dividing a graph into clusters. Hereinafter, *A* denotes the adjacency matrix of a network or graph, where *A(i,j)* represents the edge weight or affinity between nodes *i* and *j*, and *V* denotes a vertex or a set of nodes of the graph or network.

Normalized section of a vertex group $S \subset V$ defined as:

$$N_{cut}(S) = \frac{\sum\limits_{i \in S, j \in \bar{S}} A(i,j)}{\sum\limits_{i \in S} \text{degree}(i)} + \frac{\sum\limits_{i \in S, j \in \bar{S}} A(i,j)}{\sum\limits_{i \in S} \text{degree}(j)}, \tag{2.65}$$

where the normalized cut of a group of nodes *S* – the sum of the weights of the edges that connect *S* to the rest of the graph, normalized to the total weight of the edges *S* and the rest of the graph $\bar{S}$. It is intuitively clear that groups with a low normalized cut are good communities because they are well connected with each other, but weakly connected with the rest of the graph.

Kernighan-Lin algorithm (*KL*). A vertex is not considered re-moved if it has already been moved in the current iteration. After a vertex has been moved, the increment for its adjacent vertices will be updated to reflect the new assignment of vertices to partitions. Although each iteration in the original KL algorithm [63] had the complexity $O(|E|\log|E|)$, further improved to $O(|E|)$ per iteration using the appropriate data structures. This algorithm can be extended to multiple separate sections, enhancing each pair of sections in a multi-user section in the manner described above.

Agglomerative/dividing algorithms [63] start at each node of a social network in its own community, and at each stage combine communities that are considered to be reasonably similar. This continues until either the desired number of communities is obtained, or the remaining communities are not too dissimilar to further merge. Partitioning algorithms work in reverse; they start with the whole network as one community and at each stage they choose a specific community and split it into two parts. Both types of hierarchical clustering algorithms often output a dendrogram, which is a binary tree where the leaves are the nodes of the network and each inner node is a community. In the case of dividing algorithms, the parent-child relationship indicates that the community represented by the parent node has been split to get the communities represented by the child nodes. In the case of agglomerative algorithms, the parent-child relationship in the dendrogram indicates that the communities represented by the child nodes have been agglomerated (or merged) to get the community represented by the parent node.

Spectral algorithms belong to the classical methods of clustering and community detection. Spectral techniques generally refer to algorithms that assign nodes to communities based on eigenvectors of matrices, such as the adjacency matrix of the network itself or other related matrices. The upper *k* eigenvectors define the nesting of the hosts as points in *k*-dimensional space, and then classical data clustering techniques such as *K*-means clustering can be used to get the final assignment of the nodes to the clusters [63]. The main idea behind spectral clustering is

that the low-dimensional representation induced by the upper eigenvectors reveals the structure of the cluster in the original graph with greater clarity.

Multilevel methods provide a powerful framework for fast and high-quality graph partitioning, and in fact they have also been used to solve many other problems [63]. The main idea is to sequentially shrink or enlarge the input graph to get a small graph. Then split this small graph and sequentially project this split back onto the original graph, refining the split at each step.

Steen van Dongen's Markov Clustering Algorithm (*MCL*) clusters graphs by manipulating the stochastic matrix or transition probability matrix corresponding to the graph [63]. In what follows, the probability of a transition between two nodes is also called stochastic flow. The MCL process consists of two operations on stochastic matrices: Expand и Inflate. Expand (*M*) — it's just *MM*, and Inflate (*M, r*) increases each entry in the matrix *M* to the inflation parameter *r* (>1 and is usually installed as 2) and then re-normalizing the columns to sum to 1. These two operators are applied alternately iteratively until convergence, starting with the original transition probability matrix.

The considered methods of identifying communities in a social network are quite effective. However, they can only be used with a relatively small number of members and networks and communities. Scaling these methods to a real social network extremely complicates the processes of calculations and identification of communities. In addition to defining the boundaries and participants of social communities, it is also necessary to determine the type and nature of social influence on the behavior of such communities. The central issue of social influence is understanding the relationship between similarities and social connections [65]. Many studies have attempted to measure social media influence and correlation from a wide variety of perspectives. Such aspects are social similarity and influence; social impact marketing, impact maximization; the model and practice of social influence through conformity, compliance and obedience, as well as social influence in virtual worlds. The presence of social influence can be determined using traditional methods.

Homophilia [65] is one of the most fundamental characteristics of social networks. This suggests that the actor on the social network tends to resemble their connected neighbors or «friends». This is a natural result, because a given actor's friends or neighbors on a social network are not a random sample from the general population.

Existential Social Impact Test. In [66], the authors try to separate social influence from internal or interfering variables by proposing a shuffle test and a back edge test. The idea behind the random test is that if social influence is not important, the timing of such activation should not depend on the duration of the action of other agents. Even though the likelihood of an agent activating may depend on his/her friends. Therefore, the data distribution and characteristics will not change even if the exact time of occurrence is changed. The idea behind the edge-shifting test is that other forms of social correlation (besides social influence) are based only on the following. Two friends often share common characteristics or are influenced by the same external variables. Thus, changing the margins will not significantly change the score for social correlation. On the other hand, social influence extends in the direction indicated by the edges of the graph, and therefore changing the direction of the edges should intuitively change the correlation score.

Tests models using tag data from Flickr and confirms social influence as a source of correlation between the actions of socially connected people [67].

Influence and action. Influence is usually reflected in changing patterns of social action (user behavior) on a social network. In the works [67, 68], the problem of studying the degree of influence on the basis of the user's historical actions was studied. Other works [69, 70] explore how social actions develop in the context of a network and how they are influenced by social influence.

Influence and interaction. In addition to the attribute and user actions, influence can also be reflected in the interactions between users [68]. Usually, online communities contain additional information about interaction with users. For example, a Facebook user has a wall page where his/her friends can post. According to the messages posted on the Wall, it can be concluded which friends are close, and which are only acquaintances. Likewise, it is possible to use Twitter followers and followers to infer the strength of a relationship.

Maximum impact in viral marketing. Social impact analysis has many practical applications. Impact maximization in viral marketing is an example of such an important application [68]. The problem is often motivated by identifying leads for marketing purposes. The goal is to minimize marketing costs and more generally to maximize profits. For example, a company may want to sell a new product through the natural word-of-mouth effect that result from interactions on a social network. The goal is to attract a small number of influential users to product adoption and subsequently trigger a large cascade of further adoption. To achieve this goal, a measure is needed to quantify the intrinsic characteristics of the user (for example, the expected profit from the user) and the network value of the user (for example, the expected profit from the users).

Thus, social influence analysis aims to qualitatively and quantitatively measure the influence of one person on others. As social media becomes more prevalent in the daily activities of millions of people, both research and practical applications on social impact will continue to grow. In addition, the size of the networks in which the underlying applications are to be used also continues to grow over time. Therefore, effective methods of social impact are in demand.

The proposed method for assessing social influence in regional communities is based on matrix models of interaction between network agents, taking into account the exposure to the influence of various government institutions and organizations, while taking into account the political activity of the participants in the process. This approach allows to get a dynamic change in the level of exposure to social influence in a timely manner. And also, to form not only a forecast of the influence of agents, but also the interaction of various agents, taking into account their formal and informal influences, the use of administrative resources, political moods of the regional society. Thus, the final sequence of steps makes it possible to significantly simplify the obtaining of integrated results of the political and social situation at the regional level.

Development of models for assessing the impact of formal and informal leaders on regional communities

Mathematical models for assessing the susceptibility to social influence of regional communities from the point of view of attitudes towards political parties can be formally set in matrix form.

The influence of elements of state institutions, media and informal leaders, and the regional society on the formation of the rating of political forces is set in a similar way.

Let's introduce into consideration the following sets of elements and their characteristics:

– $AA = \{AA_1, AA_2, \ldots, AA_k\}$ – set of state institutions of power (formal leaders). For the convenience of subsequent calculations, let's represent the set in the form of a one-dimensional vector $A = (AA_1, AA_2, \ldots, AA_k)$. For each of the elements, the level of the organizational and state hierarchy is determined, which this element occupies. For each of the levels, let's define the weight coefficient l, which takes into account the «power weight» (political weight) of the hierarchical level of the elements of state institutions. So, with a four-level model of state structure, the values of the weighting coefficient of the level are defined as $\lambda_i \in \{1, 0.75, 0.5, 0.25\}$. Thus, the higher the level of the state hierarchy occupied by this or that element, the more significant its political influence on the regional society is supposed to be (begin the numbering of levels from the highest);

– $PP = \{PP_1, PP_2, \ldots, PP_n\}$ – set of political forces (parties, blocs, movements, political parties), presented as a one-dimensional vector $P = (PP_1, PP_2, \ldots, PP_n)$. Each political force can be assigned a weight coefficient reflecting its rating – $\theta_i \in [0, 1]$;

– $IL = \{IL_1, IL_2, \ldots, IL_l\}$ – set of informal leaders of the regional community, which include: heads of enterprises, organizations, companies, criminals, cyber intruders, etc., presented as a one-dimensional vector;

– $MM = \{M_1, M_2, \ldots, M_m\}$ – set of elements of the media (media), which include: mass media (media, newspapers and magazines of the central and local level). Internet (social networks, media resources), television, radio, presented as a one-dimensional vector $M = (M_1, M_2, \ldots, M_m)$;

– $SS = \{SS_1, SS_2, SS_3, SS_4\}$ – regional community (society), represented by the set of its age groups (segments of society). The division into age groups is standard for sociology and is determined by the following age ranges (in years) (17–30), (31–60), (61–75), (76–90). Each age category of a regional society must be matched with two coefficients. The coefficient of political activity, which can be considered as involvement in social processes and, therefore, susceptibility to social manipulation – $\psi_i \in \{0.75, 1, 0.5, 0.25\}$. And the share of the corresponding age category in the total number of persons making up the regional society $W = (w_1, w_2, w_3, w_4)$.

The influence of relevant individuals and organizations (sets AA, PP, IL, MM) on various categories of regional society (set SS) can be formally represented by the matrix **IMP**. Matrix size $(k+l+m+n) \times 4$, where m – the cardinality of the set MM, l – the cardinality of the set IL, k – the cardinality of the set AA, n – the cardinality of the set PP.

As matrix elements are used values $\mu_{ij} \in \{1, 0.75, 0.5, 0.25\}$, which are considered as weights reflecting the strength of the social influence of elements of state institutions, media and informal leaders on the attitude of regional communities towards political parties. Wherein μ_{ij} can be both positive and negative (negative value denotes the negative influence of elements of state institutions, media and informal leaders on the attitude of regional communities towards political parties).

The structural diagram of the interaction between the subjects of the regional society and formal and informal leaders is shown in **Fig. 2.23**.
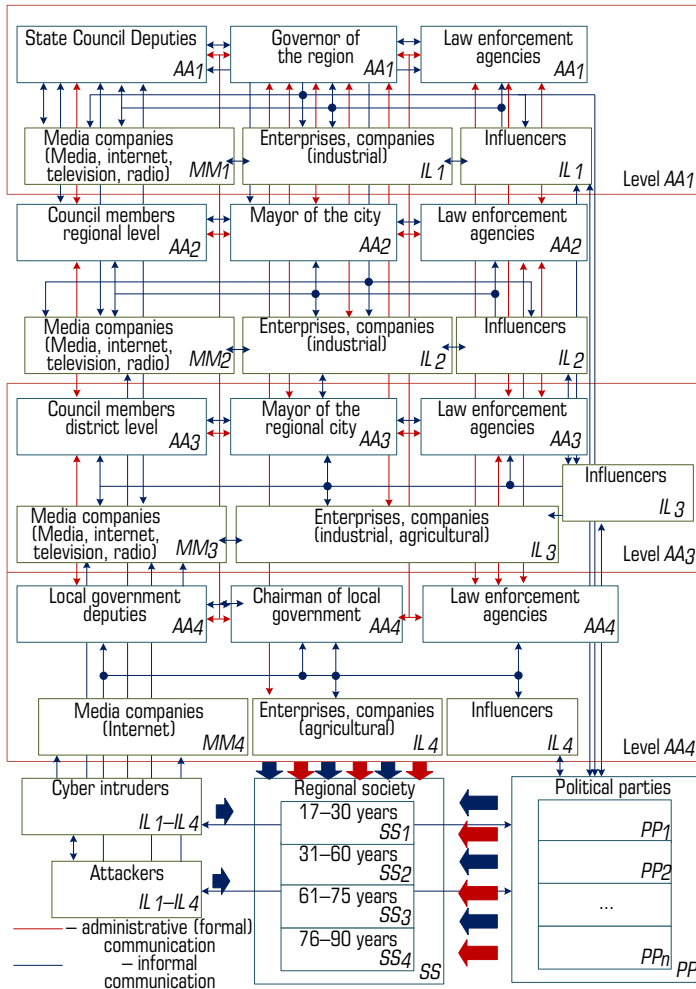
Fig. 2.23 Structural diagram of interaction between the subjects of regional society and formal and informal leaders

Let's form influence matrices for various sets that form the basis of the developed models.

Step 1. Let's form a matrix of distribution of state institutions (formal leaders) by levels of the organizational-state hierarchy:

$$H = \begin{pmatrix} h_{11} & \dots & h_{14} \\ \dots & \dots & \dots \\ h_{k1} & \dots & h_{k4} \end{pmatrix}. \qquad (2.66)$$

The number of matrix rows corresponds to the number of state institutions (formal leaders), and the number of columns corresponds to the number of levels of the public administration system (in this case, it is assumed to be 4). Element h_{ij} is equal to 1 if the state institution i is at the level j, and 0 – otherwise. Since it is possible for each institution to be at only one level, then for the formed matrix, a system of restrictions can be written:

$$\begin{cases} h_{ij} \in \{0,1\}, i = \overline{1,k}, j = \overline{1,4}; \\ \sum_{j=1}^{4} h_{ij} = 1. \end{cases} \qquad (2.67)$$

It is assumed that for state institutions their political weight (that is, the importance of the expressed opinion, point of view) is the greater, the higher the level of the organizational-state hierarchy (as a reflection of political weight). Consequently, the previously obtained values of the coefficients a_{ij}, based on the distribution over the levels of the hierarchy, should be adjusted, and will be calculated as follows:

$$h'_{ij} = h_{ij} \times \lambda_j, i = \overline{1,k}, j = \overline{1,4}, \lambda_j \in \{1, 0.75, 0.5, 0.25\}. \qquad (2.68)$$

The political weight of the respective institution is determined as follows:

$$v_i = \sum_{j=1}^{4} h'_{ij}. \qquad (2.69)$$

Formation of the vector of weight coefficients of influence on the regional society of state institutions, taking into account their hierarchical level:

$$\eta_{ij} = v_i \times \mu_{ij}. \qquad (2.70)$$

Step 2. After the formation of the value of the political weight of formal leaders, it is possible to form a matrix of the influence of the elements of state institutions of power, depending on the levels of the hierarchical model of the state:

$$h''_{ij} = h'_{ij} \times \eta_{ij}. \qquad (2.71)$$

Similar adjustments to the coefficients of influence of informal leaders and mass media can be made for the corresponding sets. However, at this stage of building the model of influence, these adjustments will not be performed and can be postponed to later stages of adjusting the model.

Step 3. Formation of the vector of weight coefficients of political activity of age groups of the regional society, taking into account the share of the corresponding age category in the total size of the regional society:

$$\sigma_i = w_i \times \psi_i, \, i = \overline{1,4}, \tag{2.72}$$

where $w_i = N_i / N_0$, N_0 – total size of the territorial community; N_i – the number of the corresponding age category of the territorial community.

Step 4. Formation of matrices of influence of formal and informal leaders, mass media, media, political parties on the regional society, taking into account its age structure, will be represented by the matrix **IMP**. Matrix dimension $(k+l+m+n)0\times4$, where k, l, m, n were previously defined as the cardinalities of sets AA, IL, MM, PP. As elements of matrix are used sets $\mu_{ij} \in \{1, 0.75, 0.5, 0.25\}$. They are considered as the weighting coefficients of the social influence of the i-th element of the set of state institutions, media and informal leaders on the attitude of the j-th age group of regional communities to political parties. Wherein μ_{ij} can be both positive and negative (negative value denotes the negative influence of elements of state institutions, media and informal leaders on the attitude of regional communities towards political parties). Influence of elements of the corresponding sets AA, MM, IL and PP on different age groups of the regional community are reflected in the corresponding matrices that form a generalized matrix of influence:

– for formal leaders:

$$\mathbf{AA} = \begin{pmatrix} \eta_{1,1} & \cdots & \eta_{1,4} \\ \cdots & \cdots & \cdots \\ \eta_{k,1} & \cdots & \eta_{k,4} \end{pmatrix}; \tag{2.73}$$

– for informal leaders:

$$\mathbf{IL} = \begin{pmatrix} \mu_{1,1} & \cdots & \mu_{1,4} \\ \cdots & \cdots & \cdots \\ \mu_{l,1} & \cdots & \mu_{l,4} \end{pmatrix}; \tag{2.74}$$

– for the media:

$$\mathbf{MM} = \begin{pmatrix} \rho_{1,1} & \cdots & \rho_{1,4} \\ \cdots & \cdots & \cdots \\ \rho_{m,1} & \cdots & \rho_{m,4} \end{pmatrix}; \tag{2.75}$$

– for political parties:

$$\mathbf{PP} = \begin{pmatrix} \theta_{1,1} & \cdots & \theta_{1,4} \\ \cdots & \cdots & \cdots \\ \theta_{k,1} & \cdots & \theta_{k,4} \end{pmatrix}. \tag{2.76}$$

A mathematical model for assessing the susceptibility to social influence of elements of state institutions, media and informal leaders on regional communities from the point of view of attitudes towards political parties is formally set and presented in **Fig. 2.24**:

$$\mathbf{IMP} = \mathbf{AA} \cup \mathbf{IL} \cup \mathbf{MM} \cup \mathbf{PP}, \tag{2.77}$$

where the matrix **IMP** – generalized matrix of the influence of various institutions on the corresponding age groups of the regional community.

Initial data

$AA = \{AA_1, AA_2, \ldots, AA_k\}$ – set of government institutions;

$\lambda_i \in \{1, 0.75, 0.5, 0.25\}$ – government level weighting factor;

$PP = \{PP_1, PP_2, \ldots, PP_n\}$ – set of political forces;

a weighting factor reflecting its rating $-\theta_i \in [0, 1]$;

$IL = \{IL_1, IL_2, \ldots, IL_j\}$ – set of informal leaders of the regional society;

$MM = \{M_1, M_2, \ldots, M_m\}$ – set of media elements;

$SS = \{SS_1, SS_2, SS_3, SS_4\}$ – regional community (society), with age ranges (in years) (17–30), (31–60), (61–75), (76–90);

$\psi_i \in \{0.75, 1, 0.5, 0.25\}$ – coefficient of political activity;

$\mu_{ij} \in \{1, 0.75, 0.5, 0.25\}$ – weight coefficients reflecting the strength of the social influence of elements of state institutions, media and informal leaders on the attitude of regional communities towards political parties

$$\mathbf{IMP} = \mathbf{AA} \cup \mathbf{IL} \cup \mathbf{MM} \cup \mathbf{PP},$$

Determination of the total intensity of the influence of the institutional structure:

additive convolution:

$$\omega_i = \sum_{j=1}^{4} \rho_{ij},$$

multiplicative convolution:

$$\omega_i = 1 - \sum_{j=1}^{4} \left(1 - \rho_{ij}\right),$$

where

$\rho_{ij} = \mu_{ij} \times \sigma_j$, $\sigma_i = w_i \times \psi_i$, $i = \overline{1,4}$, $w_i = \dfrac{N_i}{N_0}$,

N_0 – total size of the territorial community;

N_i – the number of the corresponding age category of the territorial community

Determination of the total intensity of influence on age groups:

additive convolution:

$$\tau_j = \sum_{i=1}^{k+l+m+n} \rho_{ij}$$

multiplicative convolution:

$$\tau_j = 1 - \sum_{i=1}^{k+l+m+n} \left(1 - \rho_{ij}\right)$$

In the range from $k+1$ to $k+l$ – informal, ranging from $k+l+1$ to $k+l+m$ – media, and ranging from $k+l+m$ to $k+l+m+n$ – political forces

Fig. 2.24 Mathematical model for assessing exposure to social influence

Matrix **IMP** is formed by appending the rows of the next matrix to the existing one. As a result, will be formed a matrix with the dimension $(k+l+m+n)\times 4$. In it, lines in the range from 1 to k correspond to formal leaders.

In the range from $k+1$ to $k+l$ – informal, ranging from $k+l+1$ to $k+l+m$ – media, and ranging from $k+l+m$ to $k+l+m+n$ – political forces:

$$\textbf{IMP} = \begin{pmatrix} \textbf{AA} \\ \textbf{IL} \\ \textbf{MM} \\ \textbf{PP} \end{pmatrix} = \begin{pmatrix} \eta_{11} \cdot \sigma_1 & \dots & \eta_{14} \cdot \sigma_4 \\ \dots & \dots & \dots \\ \eta_{k1} \cdot \sigma_1 & \dots & \eta_{k4} \cdot \sigma_4 \\ \mu_{k+1,1} \cdot \sigma_1 & \dots & \mu_{k+1,1} \cdot \sigma_4 \\ \dots & \dots & \dots \\ \mu_{k+l,1} \cdot \sigma_1 & \dots & \mu_{k+l,1} \cdot \sigma_4 \\ \rho_{k+l+1,4} & \dots & \rho_{k+l+1,4} \\ \dots & \dots & \dots \\ \rho_{k+l+m,4} & \dots & \rho_{k+l+m,4} \\ \theta_{k+l+m+1,1} \cdot \sigma_1 & \dots & \theta_{k+l+m+1,4} \cdot \sigma_4 \\ .. & \dots & \dots \\ \theta_{k+l+m+n,1} \cdot \sigma_1 & \dots & \theta_{k+l+m+n,4} \cdot \sigma_4 \end{pmatrix}. \qquad (2.78)$$

Thus, the developed mathematical models make it possible, on the basis of an expert assessment, to obtain an objective reflection of the influence of individual CPSS groups, their relationship and influence on the regional society. For the correct assessment of experts, let's use the mathematical apparatus proposed in [71].

Development of a method for assessing the total intensity of the influence of a particular institutional structure

The method for assessing the total intensity of influence is formed on the basis of a mathematical model for assessing the susceptibility to social influence of elements of state institutions, media and informal leaders on regional communities and the corresponding convolution. The elements of the resulting matrix are calculated taking into account the political activity of different age groups:

$$\rho_{ij} = \mu_{ij} \times \sigma_j. \qquad (2.79)$$

Step 5. The calculation of the total intensity of the influence of a particular institutional structure (formal or informal leader, political party, mass media) can be presented as a convolution by row (for all age categories):

– for additive convolution – $\omega_i = \sum_{j=1}^{4} \rho_{ij}$;

– for multiplicative convolution – $\omega_i = 1 - \sum_{j=1}^{4} \left(1 - \rho_{ij}\right)$.

Step 6. Similarly to the 5th step, the calculation of the intensity of social influence on a particular age group can be performed:

– for additive convolution – $\tau_j = \sum\limits_{i=1}^{k+l+m+n} \rho_{ij}$;

– for multiplicative convolution – $\tau_j = 1 - \sum\limits_{i=1}^{k+l+m+n} \left(1 - \rho_{ij}\right)$.

The structural diagram of the method for assessing the total intensity of the influence of a particular institutional structure is shown in **Fig. 2.25**.
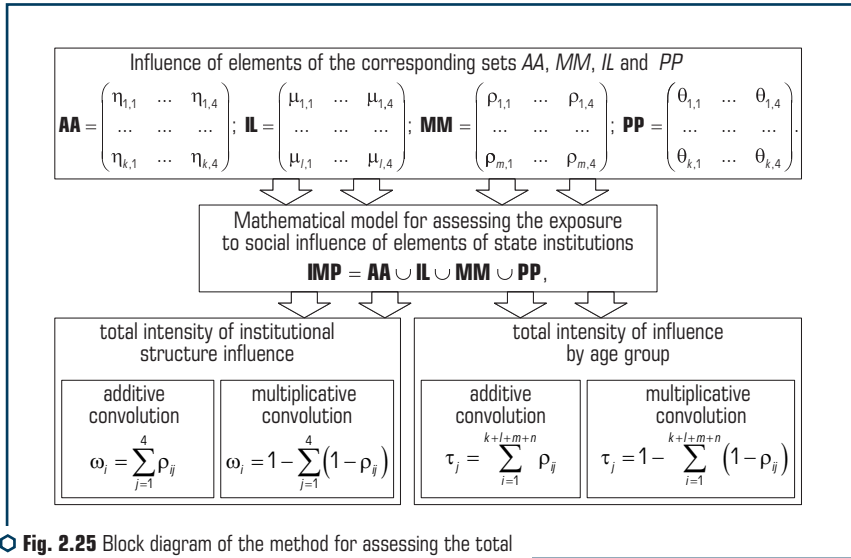
○ **Fig. 2.25** Block diagram of the method for assessing the total intensity of the influence of a particular institutional structure

This method allows, on the basis of the proposed mathematical apparatus, to objectively determine the «formal» and «informal» influence of the respective leaders on the subjects of the regional society. The basis for this is the subjective judgments of both the subjects themselves and the results of expert assessments, opinion polls, etc.

Development of a method for assessing and predicting the rating of political forces based on the mechanism of social influence

Step 7. To build a rating of political parties in the region, based on the attitude of formal and informal leaders towards them, as well as the image formed by the media, it is necessary to form a matrix for assessing political forces by the listed structures.

A mathematical model of the influence of a regional society on the formation of the rating of political forces is shown in **Fig. 2.26** and is formally set:

$$PR = \begin{pmatrix} \pi_{1,1} & \dots & \pi_{1,4} \\ \dots & \dots & \dots \\ \pi_{1,4} & \dots & \pi_{k,4} \\ \pi_{k+1,1} & \dots & \pi_{k+1,4} \\ \dots & \dots & \dots \\ \pi_{k+l,1} & \dots & \pi_{k+l,4} \\ \pi_{k+l+1,1} & \dots & \pi_{k+l+1,4} \\ \dots & \dots & \dots \\ \pi_{k+l+m,1} & \dots & \pi_{k+l+m,4} \end{pmatrix}. \tag{2.80}$$

The presented model in **Fig. 2.26** allows predicting the rating of political parties in accordance with age ranges. This approach, in contrast to the mathematical model for assessing exposure to social influence, provides a «feedback» of age groups on the attitude towards party forces.
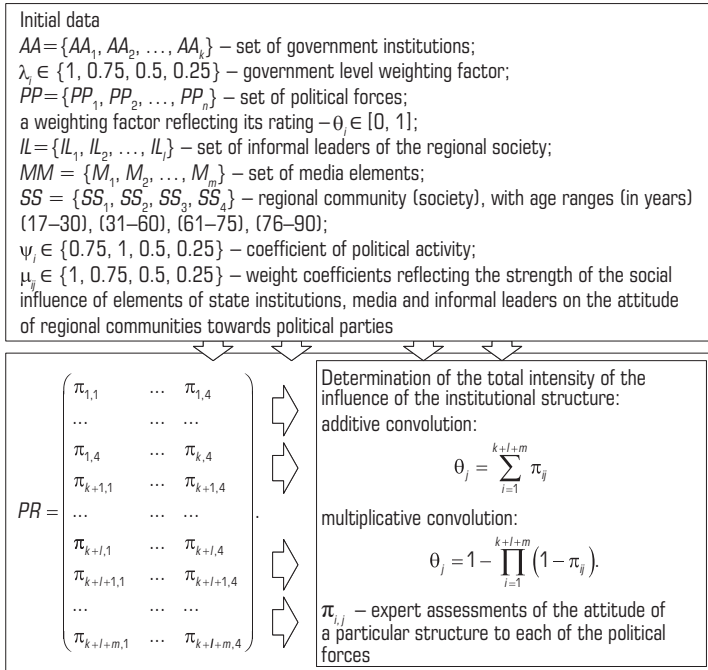
Fig. 2.26 Mathematical model, the influence of the regional society on the formation of the rating of political forces

The matrix is formed on the basis of estimates collected in the form of a table, the number of rows of which corresponds to the total number of formal and informal leaders, as well as the media (objects influencing the rating), and the number of columns corresponds to the number of political forces. Each cell of the table should contain expert assessments of the relationship of a particular structure to each of the political forces ($\Pi_{i,j}$).

The method for assessing and predicting the rating of political forces based on the mechanism of social influence is formed on the basis of the model of the influence of the regional society on the formation of the rating of political forces, as well as the corresponding convolutions.

The total score that forms the rating of a political force is obtained as a convolution of all private estimates and, depending on the selected type of convolution, has the form:

– for additive convolution – $\theta_j = \sum\limits_{i=1}^{k+l+m} \pi_{ij}$;

– for multiplicative convolution – $\theta_j = 1 - \prod\limits_{i=1}^{k+l+m} \left(1 - \pi_{ij}\right)$.

Structural diagram of the method and forecasting the rating of political forces is shown in **Fig. 2.27**.
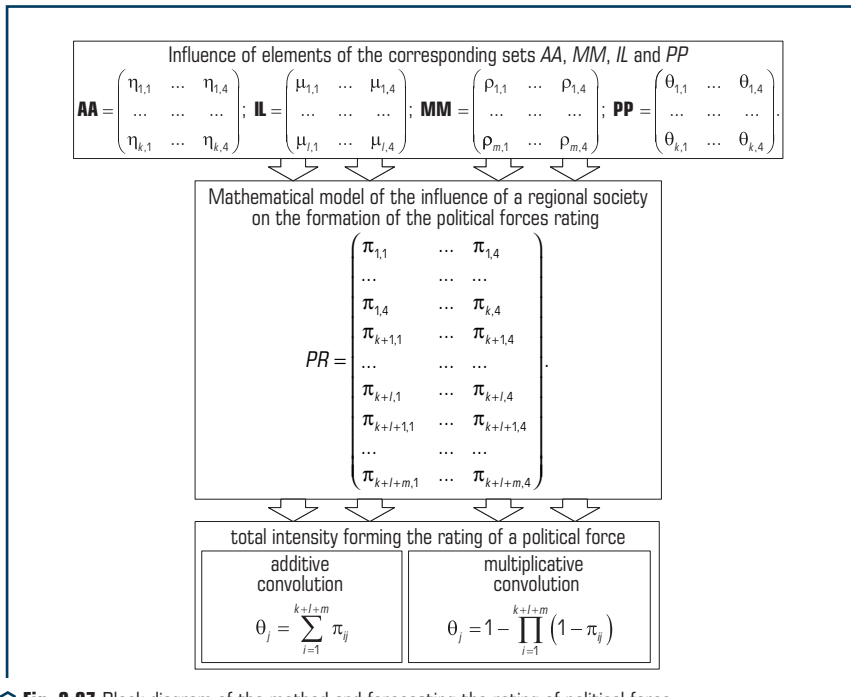
○ **Fig. 2.27** Block diagram of the method and forecasting the rating of political force

Thus, the presented approach allows one to take into account the following components:

– the hierarchical structure of state institutions and their influence on the political outlook of certain social age groups;

– electorate and influence of political parties (blocs, movements), taking into account the political worldview of certain social age groups;

– influence of informal leaders not only on political parties, but also on certain social age groups;

– the possibility of changing the rating of political parties by influencing certain elements of regional / state institutions, informal leaders and/or media.

As an example, that allows to check the performance of the proposed models and methods, as well as to discuss the results obtained, let's consider a conditionally real example. Such an example will reflect the order of interaction of the presented structures and their influence on the formation of the rating of political parties and the assessment of the strength of political influence on the regional society.

Let's compose the PR matrix. Since all estimates are dimensionless, it makes no sense to apply coefficients leading to a dimensionless unit. Also, normalizing factors are not used at this level, since they must be taken into account in the impact assessments.

Let's assume, for definiteness, there are 4 main political forces, 4 formal leaders, reflecting different levels of the administrative and state structure, 5 most influential mass media and 3 informal leaders, whose opinion is taken into account by the regional society.

$$PR = \begin{pmatrix} 0.9 & 0.5 & 0.7 & 0.4 \\ 0.8 & 0.4 & 0.6 & 0.7 \\ 0.6 & 0.5 & 0.4 & 0.7 \\ 0.6 & 0.7 & 0.5 & 0.9 \\ 0.7 & 0.4 & 0.3 & 0.6 \\ 0.5 & 0.9 & 0.8 & 0.7 \\ 0.4 & 0.8 & 0.5 & 0.7 \\ 0.6 & 0.7 & 0.6 & 0.9 \\ 0.9 & 0.8 & 0.5 & 0.6 \\ 0.7 & 0.3 & 0.4 & 0.9 \\ 0.8 & 0.7 & 0.4 & 0.9 \\ 0.5 & 0.8 & 0.6 & 0.7 \end{pmatrix}.$$

When using additive convolution, let's obtain estimates for each of the 4 political forces: $P_1 - 8.0$; $P_2 - 7.5$; $P_3 - 6.3$; $P_4 - 8.7$. Thus, the rating of political forces is as follows: $P_4 \rightarrow P_1 \rightarrow P_2 \rightarrow P_1$.

If multiplicative convolution is applied, the rating will be as follows: $P_4 \rightarrow P_1 \rightarrow P_2 \rightarrow P_1$. As can be seen, the rating did not change when switching from using additive convolution to multiplicative.

A promising area of further research for constructing a rating of political forces is the use of the hierarchy analysis method. This approach will allow, in contrast to the classical method, to use

the values obtained within the method to assess the spread of opinions of influencing structures, to take into account the weight of various influences on the formation of the rating. In addition, the use of the method of analyzing hierarchies will make it possible to get away from the criteria-based assessment of each of the political forces. The experts will be asked to give a comparative assessment of the attractiveness of a particular political force in the language of binary relations (i.e., in the form of pairwise comparison).

Let there be given a model of the influence of formal and informal leaders, as well as the media on the formation of the rating of political parties. On the one hand, it will be interested in the contribution of the influence of this or that subject to the general system of forming the rating of political forces. On the other hand, there is the proximity (similarity) of the influence of pairs, triples, fours, etc. of subjects on the formation of the rating.

To solve these problems, let's use the method of differentiating models. It should be noted that the method was presented to be used as a starting point for a matrix of incidents, containing as values the elements of zeros and ones, reflecting the existence of a relationship between a pair of vertices. Further, it is proposed to use this method in the case when the connections between the vertices are weighted, and the weight reflects the corresponding force of influence or the assessment of the corresponding object.

As a starting point, let's use the *PR* matrix presented earlier.

The intensity of participation of a particular structure in the general system of social influence (as an example, the formation of a rating of political forces), let's use the concept of a frequency matrix of relations. The frequency matrix of relations is called a square matrix, where each row (column) corresponds to one or another agent influencing the processes under consideration, and the values of the elements are determined as follows:

$$f_{ij} = \begin{cases} \text{reduced sum of the joint influence of } i\text{-th and } j\text{-th subjects if } i \neq j; \\ \text{total assessments of } i\text{-th subject if } i = j. \end{cases}$$

The frequency relationship matrix can be calculated as $PR^T \times PR \rightarrow F$ (where the superscript T indicates that the transpose matrix PR is being used).

The constructed frequency matrix of ratios based on the initial data of the experiment is presented in **Table 2.7**.

The frequency matrix of relations is an intermediate result used to derive a derivative of the model under consideration by a predicate defined as a set of subjects of influence. The elements of the specified matrix are calculated by the formula:

$$d_{ij} = \frac{\left(f_{ii} - f_{ij}\right) + \left(f_{jj} - f_{ij}\right)}{f_{ij}} = \frac{f_{ii} - 2 \cdot f_{ij} + f_{jj}}{f_{ij}}. \tag{2.81}$$

The matrix of derivatives constructed for example based on the model of the influence of the regional society on the formation of the rating of political forces is given in **Table 2.8**.

● **Table 2.7** Frequency relationship matrix f_{ij} for the model of the influence of the regional society on the formation of the rating of political forces

subjects	*j*-subject											
i-subject	1.71	1.62	1.35	1.60	1.28	1.74	1.39	1.67	1.80	1.42	1.71	1.55
	1.62	1.65	1.41	1.69	1.32	1.73	1.43	1.75	1.76	1.55	1.79	1.57
	1.35	1.41	1.26	1.54	1.16	1.56	1.33	1.58	1.56	1.36	1.62	1.43
	1.60	1.69	1.54	1.91	1.39	1.96	1.68	1.96	1.89	1.64	1.98	1.79
	1.28	1.32	1.16	1.39	1.10	1.37	1.17	1.42	1.46	1.27	1.50	1.27
	1.74	1.73	1.56	1.96	1.37	2.19	1.81	2.04	1.99	1.57	1.98	1.94
	1.39	1.43	1.33	1.68	1.17	1.81	1.54	1.73	1.67	1.35	1.71	1.63
	1.67	1.75	1.58	1.96	1.42	2.04	1.73	2.02	1.94	1.68	2.02	1.85
	1.80	1.76	1.56	1.89	1.46	1.99	1.67	1.94	2.06	1.61	2.02	1.81
	1.42	1.55	1.36	1.64	1.27	1.57	1.35	1.68	1.61	1.55	1.74	1.46
	1.71	1.79	1.62	1.98	1.50	1.98	1.71	2.02	2.02	1.74	2.10	1.83
	1.55	1.57	1.43	1.79	1.27	1.94	1.63	1.85	1.81	1.46	1.83	1.74

● **Table 2.8** Derivative matrix d_{ij} for the model of the influence of the regional society on the formation of the rating of political forces

subjects	*j*-subject											
i-subject	**0.000**	0.074	0.200	0.263	0.195	0.241	0.338	0.234	0.094	0.296	0.228	0.226
	0.074	**0.000**	0.064	0.107	0.083	0.220	0.231	0.097	0.108	0.065	0.095	0.159
	0.200	0.064	**0.000**	0.058	0.034	0.212	0.105	0.076	0.128	0.066	0.074	0.098
	0.263	0.107	0.058	**0.000**	0.165	0.092	0.054	**0.005**	0.101	0.110	0.025	0.039
	0.195	0.083	0.034	0.165	**0.000**	0.401	0.256	0.197	0.164	0.087	0.133	0.236
	0.241	0.220	0.212	0.092	0.401	**0.000**	0.061	0.064	0.136	0.382	0.167	0.026
	0.338	0.231	0.105	0.054	0.256	0.061	**0.000**	0.058	0.156	0.289	0.129	**0.012**
	0.234	0.097	0.076	0.005	0.197	0.064	0.058	**0.000**	0.103	0.125	0.040	0.032
	0.094	0.108	0.128	0.101	0.164	0.136	0.156	0.103	**0.000**	0.242	0.059	0.099
	0.296	0.065	0.066	0.110	0.087	0.382	0.289	0.125	0.242	**0.000**	0.098	0.253
	0.228	0.095	0.074	0.025	0.133	0.167	0.129	0.040	0.059	0.098	**0.000**	0.098
	0.226	0.159	0.098	0.039	0.236	0.026	0.012	0.032	0.099	0.253	0.098	**0.000**

Diagonal in **Table 2.8** is zero, which indicates a zero proximity of the influence of each of the subjects with oneself. Non-diagonal elements should be interpreted as follows: the greater the

value for a pair of subjects, the greater the discrepancy in the degree of influence of the subjects determining this value ($d_{ij} = d_{ji}$). The indicated interpretation of the matrix elements makes it possible to find subjects that have a similar influence on the processes under consideration.

Let's find the element with the minimum value. This is the element $d_{4,8}=0.005$. This means that the 4th and 8th subjects of influence have a similar nature of influence on the processes under consideration. The next most important element will be $d_{7,12}=0.012$. The found pairs can be considered as the closest in terms of the nature of the influence and, when building an aggregated model of less complexity, can be replaced by one element with the total intensity of the influence.

Thus, the proposed approach makes it possible, when analyzing the influence and formation of initial data (weight coefficients), to form an assessment of the influence of a regional society on the formation of a rating of political forces. The results obtained can be used to assess the influence of both formal and informal leaders in a particular regional society, taking into account their weighting coefficients of influence.

The main limitations of the proposed method is the subjectivity of the expert assessment of the weight coefficients, the corresponding communication lines (impact) on the corresponding elements of the proposed models for predicting the rating of political forces and the influence of a regional society on the formation of the rating of political forces. A further direction of research development is the formation of a software package that will automate the process of constructing a structural diagram of a regional society, the interaction of both formal and informal connections between the elements of the structure, as well as the possibility of analyzing the results offline.

3 METHODOLOGICAL ASPECTS OF PROVIDING INFORMATION SECURITY OF AN INDIVIDUAL, SOCIETY AND STATE IN SOCIAL NETWORKING SERVICES

ABSTRACT

The study performed a theoretical summary and proposed a new solution to the urgent scientific and applied problem: creating methodological foundations to build a system of information security in social networking services. It uses new methods to identify, assess and counteract threats to the information security of the state in the information space.

The features of the functioning of social Internet services and establishes their role in ensuring the information security of the state are analyzed. An approach is proposed to identify signs of threats in the text content of social Internet services, which will allow to quickly respond to changing situations and effectively counteract such threats.

A classifier of information security profiles of users of social Internet services has been developed to assess the level of their danger as potential participants in disinformation campaigns. A method for identifying and evaluating the information and psychological impact on user communities in services is proposed. Models of conflict interaction of user groups in social Internet services are considered on the example of civil movements. To effectively counter threats to information security of the state, it is proposed to use the concept of synergistic user interaction and self-organization processes in a virtual community. Particular attention is paid to countering the manipulation of public opinion in the decision-making process by users of social Internet services.

The obtained scientific results have a fundamental theoretical and applied practical importance for ensuring information security of the state in the social networking services and contribute to the further development of modern information technologies that implement security functions.

The digitalization of most human activities and the diversification of social communication channels became possible due to information technology development and the deepening of informatization processes. As a result, a separate class of internet platforms for communication by internet users has now emerged, formed using social structures based on the profiles of individual users or their communities. They are known as social networking services, and their users are called actors. Social networking services differ in terms of the openness to newcomers, functional characteristics, type of disseminated content, availability of additional tools for commerce, self-organization of society, management tools, and others.

The transformation of social communication processes using internet services has led to a blurring of boundaries in the virtual world between individual countries and the emergence of new threats to the information security of individuals, society, and the state. Consequently, it has become possible for perpetrators to carry out information operations aimed at a target audience to induce them to take managerial decisions and/or perform actions beneficial to the subject of information influence. Moreover, information leverage to individuals in the virtual world can become an impulse to set up or strengthen social movements and increase social tension and interethnic or inter-religious discord. Therefore, the problem of early identification, assessment, and counteraction to threats to information security of the state in social networking services is actual task.

On the one hand, in the context of new types of threats to information security emergence and the information space globalization, the practice's requirement to improve its information security when its citizens use social networking services acquires particular importance. On the other hand, there are no practical approaches to ensuring the information security of individuals, society and the state that will guarantee consistency and comprehensiveness in decision-making to counter threats in the information space. Therefore, this problem has theoretical and applied significance and needs to be solved.

3.1 SOCIAL NETWORKING SERVICES AS A COMPONENT OF THE NATIONAL INFORMATION SPACE OF THE STATE

The current state of development of the global information space characterizes by the implementation of information technology in all spheres of public activity, which creates the basis for the functioning and sustainable development of the information society [71]. However, such phenomena give rise to many systemic problems, in particular control over the information space of the state, deepening of informatization of public administration authorities and provision of public services, protection of state information resources from destructive influence, consolidation of the legal aspects of information sphere regulation. The essential place in solving the above problems is the information security of the state. Therefore, it studies the processes of ensuring the security of state interests of the country, methods of protecting individuals, society, and the state in the information sphere from external and internal threats and improving the efficiency of state information systems functioning [72, 73].

The need to protect the vital interests of individuals, society and the state is due to a close connection between the high level of intelligence and information development of society and the growing number of threats to the information security of the state. Moreover, the consequences of information influence from anywhere in the world on the citizens of a state can be the imposition of foreign interests, morals, and lifestyles to undermine the physical, material, or ideological state. In this regard, ensuring the information security of the state is an integral part of the formation of

competitive national economy functioning and sustainable development of the state in the current context of globalization and internationalization.

Information security of the state is considered with the national information space. Information space is an organized set of structures for creating, storing, and using information through a network of mass communication media to satisfy citizens' information interests and needs. An essential role in transforming national information space under independent information exchange conditions belongs to social networking services [74]. Thus, *social networking services* define services on the internet for creating user profiles, linking them with other users and virtual communities and providing tools for communication, creation, and distribution of different types of content. A user who has a profile created by a social networking service and uses it to meet information needs is an *actor*.

The primary reasons for the growing popularity of social networking services with their subsequent integration into the state information space were [73–75]:

1) equality of participants in virtual communities in cooperative social communication processes;

2) satisfaction of information needs based on one's interests and motives instead of those dictated by belonging to society;

3) lack of state influence on social networking services to form public opinion.

However, the significant limitation of state control over social communication processes in social networking services has led to their widespread use for destructive information-psychological impact on society. The vulnerability of social networking services is related primarily to the inconsistency of the level of the regulatory framework with the current level of threats to the information security of the state. Furthermore, the lack of modelling tools for the functioning of social networking services to analyze and predict their development and the insufficiency of existing measures to counteract threats increase this vulnerability level.

Global and domestic experience has shown that social networking services are associated with the emergence of new challenges to information security of the state. The first references to social networking services to influence the authorities are related to youth protests against parliamentary elections in Moldova in April 2009. Substantial discrepancies between social polling data and officially announced election results brought thousands of people to the streets of Chisinau. Facebook and Twitter were used to spread calls for participation in the protests, especially under the hash-tag #*pman* (Piazza Marii Aduneri Nacionale – the main square in Chisinau). This hash-tag appeared with posted news on *Twitter* about the developments of the situation [76, 77]. Thus, participants used social networking services to coordinate the protesters' actions. To this end, calls to unite the opposition, information on the actions of law enforcement agencies, the condition and number of people injured in clashes with the police, data on the locations of the actions, and others, were published. In addition, after the authorities blocked cellular communications, protesters used the mobile internet to interact and publish content on social networking services. Some messages were published in English for extensive coverage in foreign media. At the same time, videos of the events were distributed on *YouTube* [77]. As a result, these events were named the «Twitter Revolution» for the leading role of microblogging in organizing the protests.

Similar events occurred in Iran in June 2009 and involved protests against the presidential election results. In response to pogroms and protesters attacking government buildings in Tehran, the authorities imposed a harsh information blockade and conducted police raids. For this purpose, the state has blocked cellular communications, most social networking services, and foreign radio stations. At the same time, the state media only covered the unrest in the streets. Therefore, the protesters used the mobile internet and *Twitter* to communicate, exchanging photos and videos, information on new actions, lists of those arrested, data on the movement of police officers and others. In order to counter this, Iranian authorities, disguised as opposition activists, posted inaccurate content on *Twitter*. The protesters disseminated recommendations on identifying such authorities' agents and hiding their data on social networking services. They also distributed a link to an application for launching *DDoS* attacks against state information resources on *Twitter*.

In December 2010, revolutionary events unfolded in Tunisia due to citizens' dissatisfaction with the president's policies. A feature of these revolutionary events was their active coverage on the social networking services Facebook and *Twitter* [74, 76, 77]. The protesters effectively used the communication advantages of social networking services to coordinate their actions, share information about the protests in different cities and safe travel routes, and publish photos and videos of the events. As a result, social media outlets have become independent media for news and coverage of incidents in Tunisia. It should note that informing the global community while ignoring the events by the state media also took place through social networking services. The wave of national protests resulted in the president's resignation and a change of government.

The reported events in Tunisia were the start of a series of mass protests by citizens, revolutions and internal military conflicts in the countries of Central Africa and the Middle East. As a result, it became known as the Arab Spring. The protests in Lebanon, Jordan, Oman, Egypt, Yemen, Bahrain, Libya, Kuwait, Morocco, and Syria resulted in the collapse of governments or their changes and protracted civil unrest. Having summarized the chronology of the events of the Arab Spring, it is possible to present it in the form of a timeline in **Fig. 3.1**.

A common feature of the civil protests against the authorities was using social networking services to coordinate protests, activate society, spread protest sentiments, provide rapid coverage and inform the international media. In addition, it is notable that the communication of the protests took place using several social networking services simultaneously to reach a broader target audience through the dissemination of different types of multimedia content.

Social networking services became actively used in the civil protests in New York City called the «Occupy Wall Street» (September 2011) [76]. Demonstrators aimed to take over Wall Street, which houses the city's financial centre, to highlight the growing influence of corporations on the US government and call for structural changes in the economy. Protest marches also took place in other US cities and lasted for several months. The protesters' slogans appeared first on Tumblr, *Twitter*, and other popular social media has been used to attract new participants [74, 78].

Today, to counter threats to national security, some countries restrict citizens' access to social networking services. Since 2003, the Golden Shield Project has established the

so-called «Great Chinese Firewall» to filter PRC internet content. Access to *Google*, *Flickr*, *Dropbox*, *Facebook*, *Twitter*, YouTube, and partly *Wikipedia* has been restricted within the PRC, so citizens use their Chinese counterparts. However, attempts to organize citizen protests against the backdrop of the Arab Spring have shown that it is difficult to fully control the flow of information at the state level due to the ever-increasing number of internet users. As a result, social networking services' permanent or temporary blocking also exists in North Korea, Iran, Pakistan, Vietnam, Saudi Arabia, Egypt, Turkey, and other countries.

Analysis of the revolutionary movement in the CIS states, aimed at the non-violent overthrow of the government with a change of political regime and dubbed «coloured revolutions», links its emergence to globalization processes, development of progressive information technologies, achievement by the society of a given level of science, economy, mass media and others. The peculiarity of coloured revolutions is the peaceful nature of protests, which can later develop into bloody clashes. Thus, according to A. Hromova, the «colour revolutions» are characterized by communication, creating information pressure on the authorities. A time chart of «colour revolutions» in the post-Soviet states shows that they have occurred since 2000 (**Fig. 3.2**). The assessment of the Orange Revolution in Ukraine in 2004 points to the critical role of mobile phones in communication during the events. The rapidity of information dissemination relied on the internet, with the planning of protests conducted online in a live conversation between participants. In addition, individual ISPs provided users with free internet access, particularly opposition media websites.

Foreign experts were engaged in organizing the Orange Revolution to develop an information strategy, brands and support websites with content dedicated to the revolutionary events. Campaigning materials posted on the internet were printed and distributed to citizens in the regions. The authorities took measures to block information resources, but their owners changed their addresses or created mirror copies. Social networking services provided a leading role in the organization and conduct of the 2013–2017 Dignity Revolution in Ukraine. Primarily, social networking services helped to mobilize society to participate in mass protests and coordinate the actions of citizens, public leaders, and politicians. Thus, on November 21, 2013, according to *Watcher* [79], the number of visits of actors from social networking services to the website of the *Ukrainian Pravda* newspaper increased by six times compared to the average number of visits in that month (**Fig. 3.3**).

At the same time, there was a change in the content structure of social networking services. Actors not only disseminated statements by Ukrainian and foreign politicians related to civil protests but also became involved in its creation. Consequently, the actors were not ordinary observers of the revolutionary events but became civil activists. At the same time, the actors of virtual communities in social networking services participated in volunteer activities, charity, organization of self-defense and counteracting power structures during mass protests [79, 80]. The main consequences of the Revolution of Dignity include significant political and societal changes in Ukraine, the gradual withdrawal from the zone of political and economic influence of the russian federation and the use of armed force in response.

Fig. 3.1 Timeline of the Arab Spring
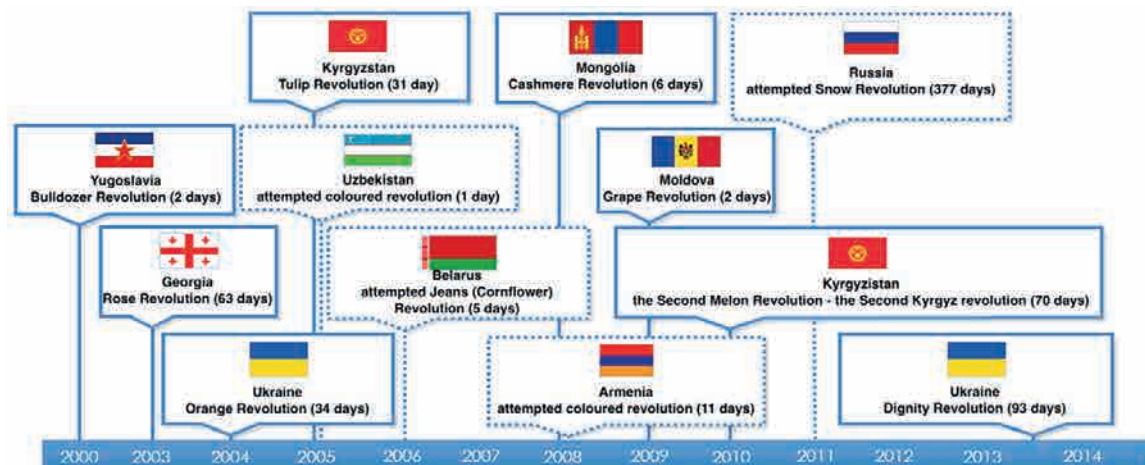
Fig. 3.2 A timeline of the «colour revolutions» in the post-Soviet states
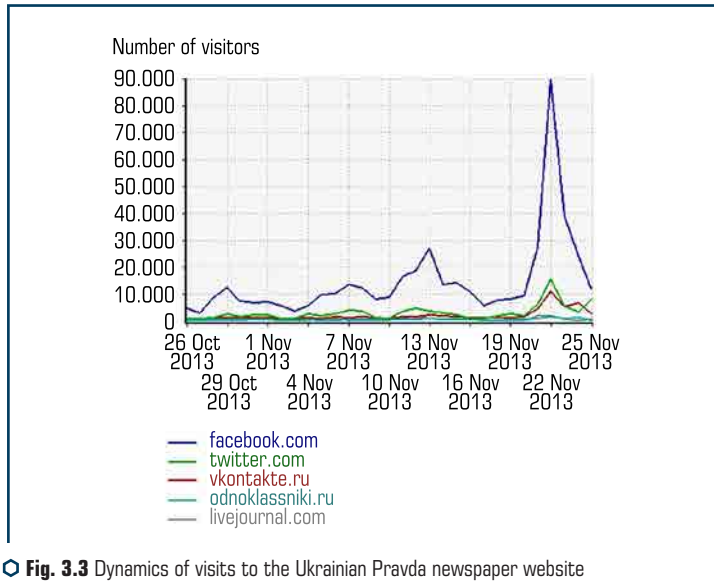
Fig. 3.3 Dynamics of visits to the Ukrainian Pravda newspaper website
by actors of social networking services at the beginning of the Dignity Revolution [17]

The events of the annexation of Crimea and the armed aggression of the russian federation in eastern Ukraine have shown that social networking services were actively used in the preparatory stages immediately during their conduct. For instance, studies [80, 81] of the information support for the annexation of Crimea in March 2014 demonstrated the use of social networking services in the russian federation's propaganda activities. According to American analyst M. Galloway, published for the US military publisher *Realcleardefense* [81], the russian federation government spent $19 million to fund the activities of 600 specially recruited actors from *Facebook*, *Vkontakte*, *Odnoklassniki*.

The activities of these actors consisted of publishing articles and comments on them to create an opinion in Ukrainian and international society that the local population supported the annexation, discrediting the local opposition and spreading rumours, feelings of fear and hate among the population. The first publications of russian information operations appeared on *Facebook*, but *Vkontakte* was the most popular, with content spreading at 5,000 reposts per day. Such content held techniques to manipulate public opinion to increase the audience of influence from older generations to young people, polarizing society. In addition, social networking services helped to legitimize the results of the pseudo-referendum on the status of Crimea. Also, in Crimea, russian information operations forces created an information vacuum by blocking government websites and conducting cyber-attacks on media websites. The result of such actions was to gain a significant advantage in the information space to facilitate actions to annex

the peninsula. Thus, the annexation of Crimea served as a test case for information operations against the information security of the state and demonstrated that social networking services are an effective tool for managing society.

In April 2014, pro-russian activists began seizing administrative buildings in Donbas. At the same time, the activity of specially created virtual communities in social networking services, primarily *Vkontakte*, intensified. The topic of such virtual communities as Antimaidan, *Novorossiya*, *Russkaya Vesna* and many others were dedicated to the ideas of *Antimaidan* and consisted of developing an alternative to the civil protests of the Dignity Revolution. However, these virtual communities disseminated inaccurate information and widely used techniques to manipulate public opinion, and their activities were purposefully imposed on actors of social networking services. One of the tasks was to disseminate propaganda materials and symbols of quasi-state formation to legitimize it in society and regional discord, aiming to create a new artificial national identity different from the Ukrainian one [81]. The purpose of information operations against the information security of an individual, society, and the state in social networking services during the armed aggression of the russian federation in Eastern Ukraine was destructive information influence on the consciousness of actors, dissemination of set ideological and social settings, development of set stereotypes of behaviour, desired transformation of public moods, feelings, will [81].The paper by B. Perry [82] analyzed the tools used by Russia during the hybrid war with Ukraine and determined that the most effective of them was information operations. Control over the escalation of the situation became achieved through active prolonged pro-russian propaganda among the population of the south-eastern regions of Ukraine. The consequences of such actions were the population's perception of the relevant narrative and the formation of a pro-russian initiative majority, which became the basis for the consolidation of separatists and support for the intervention of armed formations. Statistical data on the use of social networking services in Ukraine and the world as of July 2016, according to the company *Adpro* [83], are presented in **Fig. 3.4**.

Analysis of **Fig. 3.4** shows that russian services have a significant share of the social networking services market in Ukraine, unlike the rest of the world. On 15 May 2017, the President of Ukraine signed a decree enacting the decision of the National Security and Defense Council of Ukraine «On the application of personal special economic and other restrictive measures (sanctions)» [85]. This regulatory document prohibits Internet service providers from accessing *Odnoklassniki*, *Vkontakte* social networking services, and other russian resources. This document has led to a significant redistribution of users among other social networking services; in particular, according to Watcher, the audience of Facebook grew to 9 million users in August 2017 and Instagram to 6 million users.

It is helpful to summarize the processes of russian information operations in Ukraine in terms of patterns (**Fig. 3.5**). One of the results of information operations in Ukraine has been the creation of significant obstacles to managerial decision-making at the regional and state levels [77]. Therefore, social networking services played a leading role in organizing the annexation of the Crimea and fomenting public hostility and escalating violence in eastern Ukraine.
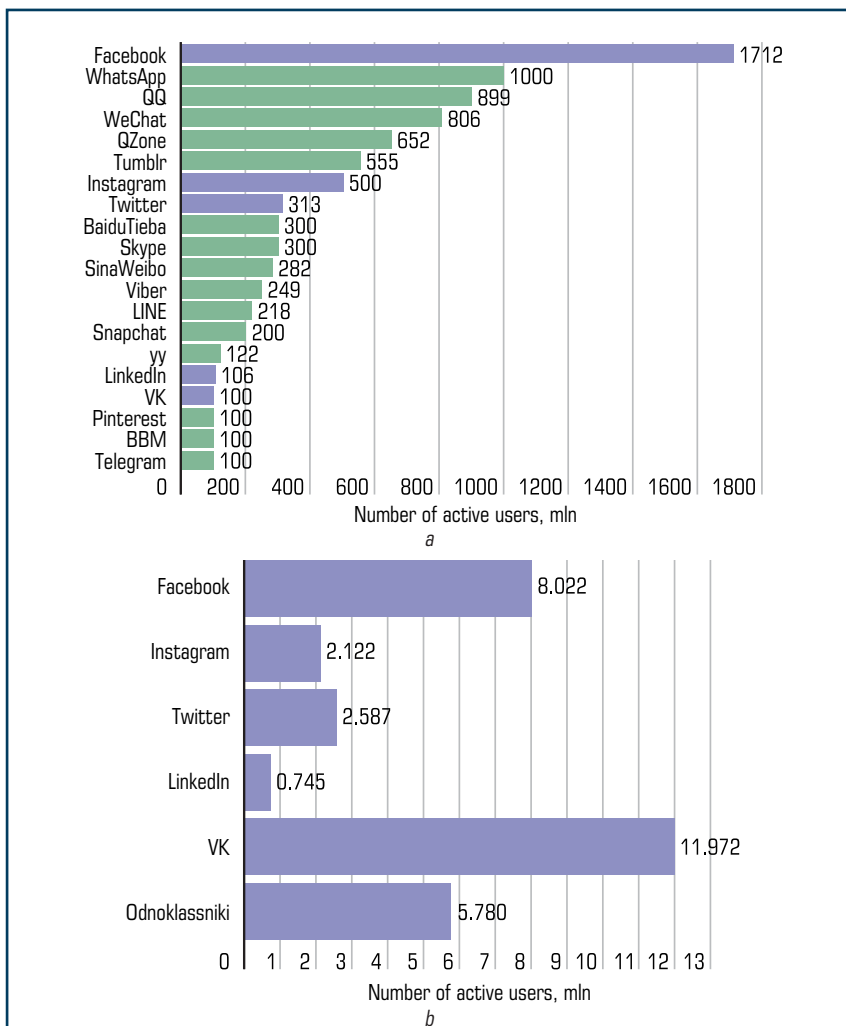
○ **Fig. 3.4** Statistics on the use of services: *a* – worldwide; *b* – in Ukraine (excluding the temporarily occupied territories of Luhansk and Donetsk regions and Crimea)

Consequently, from the scientific and technical analysis of the importance of social networking services in the process of ensuring information security of the state, it follows that:

– at the present stage of implementing progressive information technologies in public activities, social networking services represent one of the most popular means of mass communication.

Social networking services combine a broad class of tools for information interaction, which provides not only to meet the information needs of actors but also for their self-expression, education, self-development, implementation of business start-ups, so they are an integral part of the information space;

— social networking services are objects of information security of the state. Due to their communication advantages, they have become an effective tool to influence political and social processes in the state. As a result of the dissemination of inaccurate or distorted content in social networking services, together with information and psychological impact on actors in society, tensions, ethnic and religious hatred, and dissatisfaction with the political situation in the state can arise.
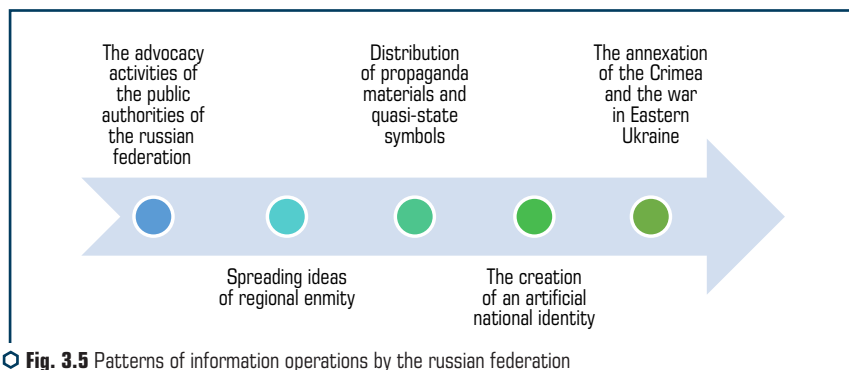
○ **Fig. 3.5** Patterns of information operations by the russian federation in the initial stages of hybrid warfare in Ukraine

Therefore, ensuring the information security of the state in social networking services in the context of globalization of the information space and hybridization of military conflicts remains one of the urgent problems that need to figure out in Ukraine and the world.

3.2 IDENTIFICATION OF THREATS TO THE INFORMATION SECURITY OF THE STATE IN THE TEXT CONTENT OF SOCIAL NETWORKING SERVICES

Today, social networking services provide users, commonly referred to as actors, with tools to create and distribute multimedia content, organize actors in a virtual community, and coordinate their interaction in real life. Therefore, social networking services effectively influence the state governance processes directly related to the information security of an individual, society, and state [73]. However, in light of recent events in Ukraine and worldwide, social media is a tool for information operations due to the purposeful dissemination of misleading or distorted content and negative propaganda. Such actions are incitement of public discord, aggravation of social conflicts, growth of protest sentiments, and interethnic and inter-ethnic discord. Therefore, one of the

essential tasks of the information security of the state system is timely identification of content in social networking services, which includes destructive information influence on actors and poses a threat to the information security of the state. Therefore, the problem of detection of threats to the information security of the state in the text content of social networking services is related to the existence of an objective contradiction between the practice and the theory. This contradiction is associated with the development of modern technologies of information influence on actors and the scientific basis of their detection based on the content analysis of natural language text. At the same time, this problem is not limited to linguistic analysis of textual content and applies, in particular, to information retrieval tasks. Thus, the complexity of procedures for early detection of threats to the information security of the state in the textual content of virtual communities is due to the lack of a comprehensive approach to their search and detection. Therefore, the development of practical approaches to the detection of information impact on actors in social networking services based on the analysis of the content of textual content is an urgent scientific and applied task.

Based on the analysis results, it is necessary to develop an approach to identify threats to the information security of the state in the textual content of social networking services for timely detection of destructive information impact on actors of virtual communities. Such an approach should increase relevance to the studied textual content of social networking services, revealing known semantic templates of threats to information security. Also, it should fill ontological knowledge bases with unknown templates of threats and feasibility in the conditions of limited resources of the security system.

Critical analysis of publications on the direction of the study showed that the processing of natural texts used statistical or linguistic analysis [84–86]. The essence of statistical methods is to analyze the content of textual content based on the frequency of use of individual words or Bag of Words. However, this approach does not allow to consider the coherence of textual content, which is one of the critical requirements for the effectiveness of detection of threats in the content textual content having a hidden nature. Therefore, to solve the task at hand, it is necessary to use linguistic analysis techniques to identify the structural and semantic coherence of textual content, communicative focus and interpretation to establish meaning. The linguistic analysis consists of several main stages, among which semantic analysis is the most interesting for research. The semantic analysis procedure relies on knowledge bases and thesauri and shows the relationship between individual words and phrases in the textual content. It also establishes that the problem of identifying threats to information security of the state in the textual content of social networking services relates to the use of information retrieval methods [87]. Therefore, applying semantic search and analysis methods to consider the content of the textual content of virtual communities is promising.

A peculiarity of the social networking services functioning is the use of such architecture of content dissemination, which influences the emotional sphere of actors. Thus, the publications of actors or virtual communities are publicly available and cause other users of social networking services to show emotional appreciation of such content in the form of comments, likes, and reposts. The use of covert information influence on actors combined with manipulative influence techniques leads to

manipulation of public opinion. Based on the results of the report *Information disorder: toward an interdisciplinary framework for research and policymaking* [88], it establishes that the exercise of information influence in social networking services bases on the following constitutive concepts:

1) three types of information influence – misinformation, incomplete content, malicious content;

2) three stages of information impact – creation, production, consumption;

3) three components of information impact – actor, content, interpretation.

The considered components of information impact form a conceptual model consisting of a set of relevant concepts. Each of the concepts defines the corresponding variable describing the state of the corresponding concept. At the same time, individual concepts represent objects of information space of social networking services, affecting the information security of an individual, society and state.

Fig. 3.6 shows the interconnection of the considered components of information influence in social networking services.
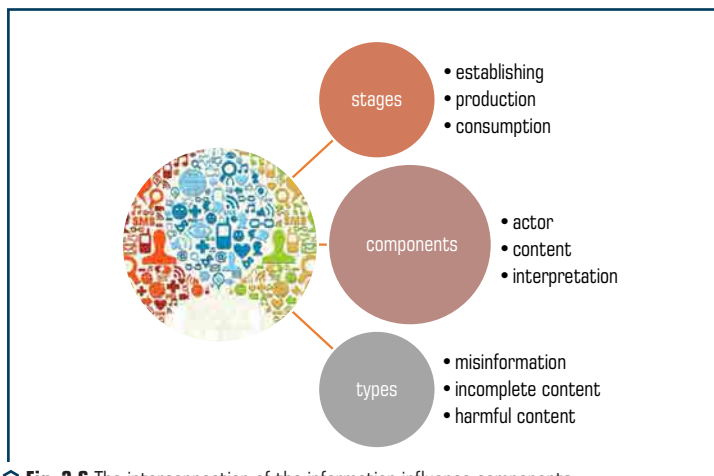
○ **Fig. 3.6** The interconnection of the information influence components

The conceptual model is summarized in **Table 3.1**.

Thus, the information influence on actors of social networking services described by the proposed conceptual model allows the development of a systematic model for identifying threats to the information security of the state in the textual content.

Using a systematic approach to identifying information influence on actors of virtual communities in the textual content allowed to implement a comprehensive approach to finding and identifying threats to information security of the state in the social networking services.

For this purpose, a systematic model of detection of threats to information security of the state in the textual content of social networking services is proposed, presented in **Fig. 3.7**.

● **Table 3.1** Characteristics of the conceptual model

Multiple concepts	Variable states	Note
$X^{type} = \left\{ X_i^{type} \right\}$	Y_i^{type}	Types of informational influences in social networking services: *disinformation* – deliberately created artificial content intending to have a destructive impact on actors, a group of actors, society, and the state; *incomplete content* – content insufficient for informed decisions on the completeness, with no destructive impact on actors; *malicious content* – content based on facts aimed at causing harm to an actor, a group of actors, society, and the state
$X^{phase} = \left\{ X_i^{phase} \right\}$	Y_i^{phase}	Stages of information impact: *creation* – this boils down to the development of a narrative for further informational impact on a particular target audience; *production* – consists of creating content that contains informational impact on actors, either explicitly or implicitly; *consumption* consists of distributing and publishing content containing information that influences social networking services
$X^{comp} = \left\{ X_i^{comp} \right\}$	Y_i^{comp}	The components of information impact: *actor* – a user who satisfies information and communication needs using social networking services; *content* – information content of virtual communities of social networking services for the interest of actors, expression of a point of view on current events, dissemination of prompt and helpful information; *interpretation* – the actors' interpretation of the consumed content, their reaction to it, and actions in virtual or real space due to the information impact
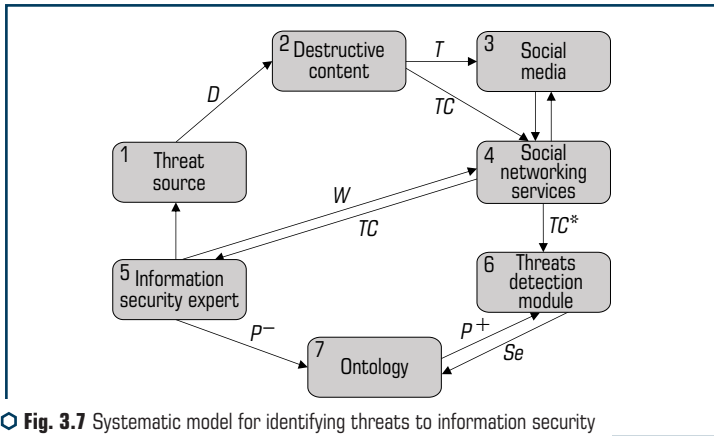
○ **Fig. 3.7** Systematic model for identifying threats to information security of the state in the textual content of social networking services

The source of threats to information security of the state is characterized directly by threats D_j, $j = \overline{1,k}$, formalized using a cortege:

$$D = \langle R,S,C,T,Sph,M,F,Sr,Pos,I \rangle,$$

where R is the relation of the threat to actors on social networking services; S is the type of threat actor; C is the nature of the threat with social networking services; T is the purpose of the threat realization; Sph is the sphere of social activity affected by the threat; M is the way the threat acts; F is the frequency of recurrence; Sr is the covert manifestation; Pos is the possibility of the threat realization on social networking services; I is the level of influence on actors in social networking services.

The development of informational influences on actors in virtual communities, taking into account the relevance, level of discussion and public-criticality of informational issues in the media, results in the formation of appropriate textual content:

$$TC = \{TC_i\}, \, i = \overline{1,n}.$$

The content is then disseminated in the media and social networking services to influence public opinion. An information security of the state expert forms a semantic kernel based on an analysis of the information space of social networking services:

$$W = \{w_m\}, \, m = \overline{1,l},$$

to search for textual content on a given information issue related to the need to protect national interests. The selected textual content:

$$TC^* = \{TC_b^*\}, \, b = \overline{1,d},$$

goes to the threat detection module of the information security system of the state in social networking services.

The study of TC^* textual content for informational impact on actors in virtual communities takes place using an ontology for semantic analysis. Semantic patterns of known threats to information security of the state identified as:

$$P^+ = \{Pattern_z^+\}, \, z = \overline{1,r}.$$

If the selected TC^* textual content is highly relevant and contains no known semantic threat patterns P^+, it goes forward for further investigation by an information security of the state expert. If new unknown threat patterns are detected:

$$P^- = \{Pattern_z^-\}, \, q = \overline{1,v},$$

they complement the universal set of semantic threat patterns $P^\pm$.

The proposed approach to identifying threats uses a method for detecting information impact on social networking services based on the content characteristics presented in [15]. As a result of the research, it found that a promising area of improvement is the use of weighted semantic kernel components to increase the relevance of selected content and its further analysis for threats to the information security of the state. Thus, the essence of the proposed approach is as follows.

Step 1. Search for textual content in social networking services based on weighted semantic query components. At this stage, an information security expert defines a semantic kernel $W = \{w_m\}, m = \overline{1,l}$, to search for textual content in social networking services according to the criterion of relevance, criticality and the level of public discussion of its subject matter. Furthermore, due to the peculiarities of publishing textual content, a latent semantic indexing method (*LSI*) [87] has been used, which provides content search in social networking services based on its content rather than keyword density and finding hidden semantic links. The essence of the first step is to perform the following steps:

1.1) pre-preparing the learned content of social networking services TC^* by removing stop words, steaming or lemmatizing words. Stop words create «information noise» and are represented in natural text by conjunctions, particles, prepositions, etc. Stemming is highlighting the base of a word, excluding endings and suffixes, and is not necessarily on large sets of social media content publications. Lemmatization is the reduction of a word to a lexical form;

1.2) eliminating words used only once from the textual content of social networking services;

1.3) forming an indexed frequency matrix of M keywords W. The rows of this matrix i are the keywords W of the semantic kernel followed by monitoring the textual content of social networking services, and the columns j are the publications of actors of virtual communities. The matrix elements m_{ij} represent the frequency of use of some keyword w_i in the j-th publication;

1.4) consists of a singular decomposition of the initial matrix M into three components:

$$M = U \times S \times V^T,$$

where U and V^T are orthogonal matrices of dimension $i \times k$ and $k \times j$; S is a diagonal matrix of dimension $k \times k$, where k is the number of singular values of the matrix (hidden content topics) and its elements have descending order;

1.5) those matrix rows U and columns V^T, which correspond to the largest singular numbers k, and their magnitudes are the degree of occurrence of keywords in the collection of publications. In order to improve the efficiency of content detection with disruptive information influence, the relevance criterion of selected publications is introduced [88]:

$$RP_j = \sum_{i=1}^{m} w_{ij}\alpha_i,$$

where w_{ij} is the coefficient of the importance of the latent topic detected based on the frequency of keywords; α_i is an expert evaluation of importance.

The coefficient w_{ij} calculated according to the *Zipf* law based on the expression [89]:

$$w_{ij} = \frac{m_{ij}}{\lg D / f_j},$$

where D is the total number of publications under study; f is the number of publications where the keyword w_i appears. The expert evaluation α_i determined as the results of the conducted survey:

$$\alpha_i = \frac{1}{L}\sum_{l=1}^{L}\alpha_{lj}, \ \alpha_{lj} = \frac{\sum_{l=1}^{L}\varphi_{lj}}{\sum_{l=1}^{L}\sum_{j=1}^{D}\varphi_{lj}},$$

where φ_{lj} is the rank assigned by the *l*-th expert to the *j*-th publication.

After that, the investigated publications in social networking services are sorted based on the relevance criterion of the documents under analysis.

Step 2. Identification of signs of threats to information security of the state in social networking services based on signature method and anomaly detection method, as follows:

2.1) an ontology of virtual community functioning in social networking services is drafted:

$$Ont = \langle P_n, R_n \rangle,$$

where Ont is an ontology; P_n is a finite set of concepts; R_n is a finite set of relations between concepts.

The following subsets become distinguished in Ont ontology [86]: $P_S(p_n) \in P_n$ is a subset of the set of concepts P_n adjacent to some concept p_n; $P_{in}(p_n) \in P_n$ is a subset of the set of concepts P_n incident to relation r_n; $R_{in}(p_n) \in P_n$ is a subset of the set of relations R_n that are incident to some concept p_n; $R_z(p_n) \in R_n$ is a subset of the set of relations R_n whose use indicates danger to the concept p_n;

2.2) construction of a semantic description of the textual content found in the first stage:

$$Sem_t = \langle P_t, R_t \rangle;$$

2.3) detection of threat indicators in the pre-indexed textual content of social networking services. Formally, the rules for detecting threats to information security of the state are summarized as follows [86]:

a) signature-based detection and semantic features:

$$\exists r_t(p_t): \ p_t \in P_n \wedge r_t \in R_z(p_n),$$

where $r_t(p_t)$ is some relation from the analyzed social networking textual content; $p_t \in P_n$ is the Ont ontology concept of the virtual community under study; $r_t \in R_z(p_n)$ is the set of relations indicating a threat to some concept p_n;

b) anomaly identification bases on anomaly detection by comparing the semantic description of the indexed textual content and the semantic threat template. In doing so, a factual inconsistency in the content of social networking services is established, which manifests itself as:

– conceptual inconsistency in the content of virtual communities – the use of the concept in a particular relationship is not provided by the ontology:

$$\exists r_t\left(p_t\right):\ p_t \in P_n \wedge r_t \in R_n \wedge p_n \notin P_{in}\left(r_n\right);$$

– content relation contradiction – the used relation between concepts is not defined by the ontology:

$$\forall p_n \in P_n \neg\, \exists r_n \in R_n:\ r_t = r_n;$$

2.4) extensive review by information security of the state experts of indexed TC^* textual content for threats. This step is necessary if the content of social networking services has a high degree of relevance to the semantic core of the search query in step 1. However, in step 2 no correspondence between fragments of such content and the ontology is found. Then the new semantic threat constructs $\left\{Pattern^-\right\}$ identified by the experts supplement the universal threat set $\left\{Pattern^\pm\right\}$, which contains known threat patterns $\left\{Pattern^+\right\}$, i.e.

$$\left\{Pattern^-\right\}=\left\{pattern_i^+\,\middle|\,pattern_i^+ \notin Pattern_i^+,\ pattern_i^+ \in Pattern^\pm\right\}.$$

In line with the described approach, let's give an example of searching textual content in the social networking service Facebook without using weighted components of the semantic query kernel to prove the need for improving search efficiency. A full description of the experiment performed can be found in [86].

In the beginning, let's set the semantic kernel:

$W=<Maidan;\ bandits;\ authority;\ police;\ corruption;\ dictatorship;\ war;$

$poverty;\ Poroshenko;\ oligarchs>.$

For its search in the collection of publications D_i, $i=\overline{1,10}$ of actor Nikolai Haiduk in the social network Facebook. The results appear in **Table 3.2**.

To visualize the results of the calculations, let's show them on a graph (**Fig. 3.8**).

From **Fig. 3.8** it is possible to see that the indexed documents D_2, D_3, D_5 and D_{10}, despite the presence of words from a given semantic kernel W, are not relevant to the search query. The documents D_4, D_6, D_8 form an unobvious connection with the terms related to the «establishment of the dictatorship of the Poroshenko oligarchate». The terms «bandits», «war», «corruption» and «Maidan» are also close to the content of the documents D_1 and D_7, which bring them together

in a separate group. The document D_9 content is closely related to the low standard of living of the population and does not contain hidden dependencies from other words of the semantic core.

● **Table 3.2** Indexed word frequency matrix

Keywords	Publications									
	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8	D_9	D_{10}
Maidan	1	0	1	0	1	0	0	1	0	0
bandits	0	1	1	1	1	0	1	1	0	0
authority	1	1	0	0	1	1	1	0	0	0
police	1	1	1	0	1	1	0	0	1	1
corruption	0	0	1	1	0	0	1	1	0	0
dictatorship	1	1	0	0	0	0	1	0	1	0
war	0	0	1	0	1	0	1	1	0	0
poverty	0	0	0	0	0	0	0	0	0	1
Poroshenko	1	0	0	1	0	0	0	1	1	1
oligarchs	1	1	0	0	1	1	0	1	0	0
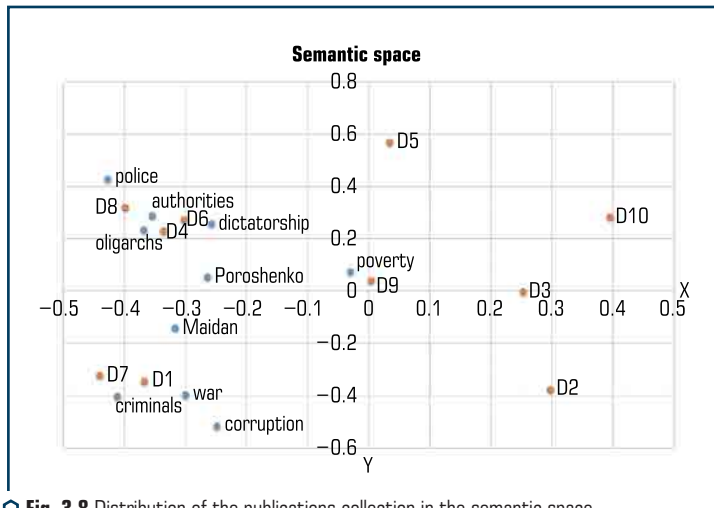
○ **Fig. 3.8** Distribution of the publications collection in the semantic space

Consequently, documents D_1, D_4, D_6, D_7, D_8 are relevant to the semantic kernel W and require further semantic analysis. By using weighted components of the semantic query kernel, the number of selected documents decreases by focusing on the topics chosen by the experts. The proposed

approach for identifying threats is discussed in more detail in [86, 89]. Thus, the total number of documents for further investigation by the content monitoring module of the information security system in social networking services decreases, and the efficiency and speed of its functioning increase.

The advantage of the proposed approach is that a combination of semantic and latent semantic analysis provides mutual compensation for their shortcomings. For example, it helps avoid polysemy, homonymy, and other linguistic ambiguities for LSI. Also, the proposed approach identifies latent dependencies between concepts for semantic analysis.

Ensuring a given state of information security of the state in the social networking services relates to detecting threats in the content of virtual communities. The proposed conceptual framework for the study of threats to information security of the state in the textual content of social networking services determines that the implementation of information impact on actors in social networking services based on such components of the type of impact, stages and components. The conceptual basis is the basis of the system model for detection of threats to information security of the state, used in developing an approach to the detection of threats in the content of textual content. The developed approach relies on the modern methods of content research – latent-semantic indexing and semantic analysis using ontologies, the combination of which provides mutual compensation of flaws and identification of hidden dependencies between language units. The proposed approach differs from the known ones by using weighted components of the semantic core of a search query to increase the relevance of the selected textual content. Ranking a collection of selected textual publications increased the efficiency of detecting threats to information security of the state. Completing a universal set of threat patterns is made with the involvement of experts on the information security of the state. In this case, research of the textual content with high relevance index in the absence of known threats provides the addition of new unknown semantic templates to the ontological knowledge base. Thus, the proposed approach to identifying threats in the textual content of virtual communities allows for improving the efficiency of the system of information security of the state in the social networking services.

3.3 INFORMATION SECURITY PROFILES OF ACTORS IN SOCIAL NETWORKING SERVICES AND THEIR CLASSIFICATION

In creating actor profiles of social networking services, users fulfill personal information in the questionnaire. Therefore, using aggregated data of an actor's profile, his/her publications in virtual communities, and the specifics of interaction with other actors is a promising area of scientific research for the construction of their information security profiles. Let's understand the information security profile of an actor in social networking services as a set of aggregated characteristics of an actor's profile in the service. The information security profile of an actor allows determining the level of his threat as a possible participant of information actions directed against the information security of an individual, society, and state [85]. However, the problem of deciding on the threat

level of actors is related to the insufficient number of profile attributes and their low informative-ness, the complexity of the procedures of automated analysis of the content of social networking services. Also, actors often provide incomplete or unreliable information about themselves for the anonymity of interaction with other subjects of social networking services, which further compli-cates building an information security profile. Therefore, the development of methods for auto-mated construction of actors' information security profiles and decision-making models for their involvement in information actions is an urgent theoretical and applied problem to solve the problem of developing an effective system of information security of the state in social networking services.

Analysis of recent studies and publications [85, 90] has shown that the attributes of actor profiles in social networking services divide into a few categories. They are numerical (age, level), categorical (marital status, profession, life values and others), and a set of specific attribute values that forms its overall characteristic. Furthermore, it has been found that machine learning methods are applied for this purpose. In particular, binary classification based on the attribute profiles of actors of social networking services is used. In addition, the gender classification tasks also apply structural attributes based on the intellectual analysis of the content published by the actor.

The team of authors in [90, 91] shows that in the general case, establishing the hidden attributes of actor profiles refers to the classical tasks of sociolinguistics – to determine the characteristic features of the language of different social groups. For this purpose, machine learning techniques with a teacher classify linguistic and other attribute actors into predefined classes corresponding to given values of attribute sets. Most of the publications on detecting latent actor attribute focus on gender detection. Scientific studies [91, 92] aim to determine the age of actors in social networking services as a continuous and discrete value. The textual content generated by an actor and stylistic attributes of this content using to establish an actor's age. Paper [90] suggests determining the po-litical affiliation, relationship to the Starbucks fast-food chain and ethnicity of actors based on profile attributes in social networking services, behavioural traits, message content and connections with other actors. To determine the geolocation of actors in social networking services, [93] uses thema-tic modelling of textual content and word distribution based on the geographical location of the actor.

Hence, in general, an actor's profile on social media contains explicit or implicit information that is sufficient to decide whether to engage him or her in information actions. Thus, there is an objective contradiction between the level of development of information technology and the scientific basis for automated threat detection in social networking services. The lack of effective methods for analyzing actor profiles for early warning of informational influences further updates is the promised field of research.

At the present stage, among the forms of information confrontation in social networking ser-vices, the following are distinguished [76]: reconnaissance, aimed at secretly extracting data and information about control in the systems of the opposing party; offensive, aimed at distorting, blocking, destroying information; defensive, carried out by the state to protect its interests. To im-plement such forms of confrontation in social networking services, actors use appropriate patterns of behaviour and interaction in virtual communities.

The experience of hybrid warfare with the russian federation has shown that specialized software is involved in social media operations, using social bots to distribute targeted content to disrupt actors. Trolls are the most aggressive type of social bots. The primary function of trolls is to post offensive and hostile comments, create arguments between actors, and maintain an information backdrop to spread a given content. However, trolls can be real people influenced by manipulative techniques or individuals who comment and distribute given content publications on social networking services on a paid basis – the so-called *Olgino trolls*. As a result of previous research, the author has developed a technology for detecting social bots proposed in [94]. In turn, the automation of actor profile analysis procedures in terms of threat to information security of the state reduced to the construction of actor information security profile. The method of building an actor's information security profile of social networking services by analyzing its attributes due to the research of M. Pennacchiotti and A. M. Popescu goes as follows.

Step 1. *Analysis of actor profile attributes*. An actor's profile attributes are an indirect source of information about his or her personality and interests. Thus, actors often indicate incomplete or unreliable information for different purposes – to create a positive image, conceal data about the personality, etc. The following attributes are essential for the task of building an actor's information security profile:

1) the name of the actor. Studies show that the names of artificially created accounts frequently repeat themselves. Also important is information about actors who have already been identified as contributors to information actions on social networking services;

2) an actor's place of birth and residence is used to establish his or her affiliation to a geographical area and to identify further patterns of behaviour and interaction in social networking services;

3) the educational institution and place of work are sources of information about the actor's qualifications and contain information about his or her geolocation.

Step 2. *Identify the characteristics of content-publishing activity*. Two categories of actors have been identified, depending on the characteristics of publishing content on their profiles. The first one usually includes actors who post content infrequently, have many friends, and are prone to seeking information, commenting on other actors' publications, and engaging in dialogue with them – so-called content consumers. The second category of actors often publishes their content or hyperlinks to third-party information resources on social media services and is referred to as content providers. Thus, establishing indicators of the frequency of publishing content of different origins, hashtags, hyperlinks, etc., and analyzing and summarizing them allows their assessment of the defined categories. Therefore, let's use the following to evaluate the indicators of activity in social networking services:

1) the total number of the actor's profile publications on social networking services;

2) the total number and share of publications that are reposts of the content of other actors' profiles;

3) the total number and proportion of comments or replies to the publications;

4) average number of hashtags and hyperlinks per publication;

5) average time between content postings and standard deviation;

6) average number of publications per day and standard deviation;

7) share of content publications by an actor in the last 24 hours.

Step 3. Identify the attributes inherent in the content of the actor's profile. The peculiarities of an actor's language, life values and sphere of manifested interest using relevant linguistic units in textual publications. Identifying such characteristic features of the content published by an actor in social networking services is a source of data for the construction of an actor's information security profile. In doing so, the textual content appears as an unrelated set of words or *Bag of Words* and the following actor profile attributes are identified:

1) characteristic words that the actor uses in his/her publications. Such words are lexical units for identifying the actor's unique attributes and assigning him/her to a given threat class. In order to detect feature words, a probabilistic model of their automated extraction based on the data of several essential actors B_i for each of the given classes c_i was used [94, 95] and consisted of the following:

– estimation of belonging of a characteristic word to a given actor class:

$$char\left(w,c_i\right) = \frac{\left|w,B_i\right|}{\sum\limits_{j=1}^{n}\left|w,B_i\right|},\qquad(3.1)$$

where w is the word used at least once by the base actors of class c_i; $\left|w,B_i\right|$ is the number of uses of the word w by all actors of class c_i; n is the number of classes.

For each class, f characteristic words of more than three characters in length are chosen with a high score;

– calculation of the coefficient linking each characteristic word chw with actor a:

$$score_{chw(a)} = \frac{\left|a,chw\right|}{\sum\limits_{w \in W_a}\left|a,w\right|},\qquad(3.2)$$

where $\left|a,chw\right|$ is the number of times the actor a uses the characteristic word chw; W_a is the total number of words used by the actor a;

– calculation for each class a coefficient, putting the actor's function:

$$score_{c(a)} = \frac{\sum\limits_{chw \in ChW}\left|a,chw\right|}{\sum\limits_{w \in W_a}\left|a,w\right|},\qquad(3.3)$$

where ChW is the set of characteristic words for class c;

2) identification of common interests of basic actors of the same class based on latent topics of the published content. For extracting hidden information in the actor profile content, it is reasonable to use probabilistic thematic modelling techniques and probabilistic latent semantic

indexing (*PLSI*). This method asserts that the occurrence of words *t* in publications *d* results from variables *z* representing the content's latent (hidden) subject matter. In our case, the latent content topics of the actors represent their interests, and the probabilistic model of the occurrence of the pair (*d*, *t*) takes the form:

$$P\left(d_m, t_m\right) = \sum_{k=1}^{l} P\left(z_k\right) P\left(d_m \middle| z_k\right) P\left(t_n \middle| z_k\right),$$

(3.4)

where $P(z_k)$ is the distribution of topics over the collection of publications; $P\left(d_m \middle| z_k\right)$ is the probability that publication d_m belongs to the group of publications of topic z_k; $P\left(t_n \middle| z_k\right)$ is the probability that word t_n belongs to the word group of topic z_k;

3) characteristic hashtags used by the actor. Hashtags are used in social networking services to group actors' publications into groups, simplify the search for content on a given topic and consist of one or more words and are denoted by the symbol #. Actors of social networking services with common interests use similar hashtags, so it is reasonable to form a set of characteristic hashtags for basic actors similar to characteristic words. To do this, expressions (3.1) to (3.3) apply;

4) tone of the content published by the actor. In some cases, an indicator of an actor's membership in a particular threat class is the tone of the content according to a given set of words. Among such words are those related to national security issues, such as political structure, territorial integrity, etc. The tone of the content profile of an actor takes the meaning of «positive», «negative» and «neutral». For tone analysis, it is advisable to use supervised machine learning methods [96, 97], whose advantages are high accuracy and speed, the efficiency of automation of content analysis procedures, assignment of content to predefined tone classes, and availability of accuracy assessment tools. After analyzing the tone of the content, the following indicators are calculated:

– positive, negative and neutral tone content particles;

– mean value and standard deviation of tonality for the whole given set of words;

– the number of given words about which the actor has a negative, positive or absent point of view.

Step 4. *Analyze the actor's connections.* Informative attributes of an actor's profile in social media are his/her connections with other actors and virtual communities, his/her mentions in messages or content distribution. Therefore, to analyze an actor's connections in social networking services, let's consider the following attributes of his/her profile:

1) the total number of friends, followers and virtual communities of the actor. These indicators allow to conclude the purpose of using social networking services in terms of information exchange. If the actor has many friends and is a member of many virtual communities, he/she is a content consumer. If the actor has a large number of followers and frequently publishes content, then he/she is a content provider;

2) a feature of the actor's friends' profiles and virtual communities. The actor's interests appear in the choice of friends in the social networking services and virtual communities in which he/she participates. Such mechanisms in services are known to organize interaction between actors with shared interests and opportunities for self-organization in real life. To analyze the features

of actor's connections, let's use the principle of character word detection of stage 2 of this method and equations (3.1)–(3.3). To do this, let's select profiles of popular actors who are opinion leaders, famous figures, etc. and use them as the base;

3) content distribution of friends and virtual communities. Similarly, to analyze the specifics of the actor's connections in the previous paragraph, let's investigate the sources which content he/she cites. Depending on his/her interests, the actor disseminates content corresponding to his/her interests. Therefore, it is helpful to identify the base actors and virtual communities for each threat class and use equations (3.1)–(3.3) to assign the actor to one of these groups.

Step 5. *Determine the threat class*. After assessing all the characteristics of the social Internet actor profile, it is necessary to assign it to one of the threat classes $Y = \{$*very high*; *high*; *significant*; *tolerable*; *low*$\}$.

For this purpose, teacher-assisted machine learning techniques perform classification into predefined classes. Effective for classifying actors by threat level are methods that rely on binary classifier boosting procedures. The essence of boosting is to build a composition of machine learning algorithms, where each successive algorithm compensates for the shortcomings of the composition of all previous algorithms. In the case of multiclass gradient binary classification on decision trees on Q classes, let's set the loss function as [98]:

$$L = -\sum_{q=1}^{g} y_g \log p_q(x),$$ (3.5)

where y_g represents the object belonging to class q; p_q is the probability of the object belonging to class q as a result of logistic regression.

Then the final classifier takes such form:

$$q(x) = \text{argmin}_{q \in [1,Q]} \sum_{\tilde{q}=1}^{K} c(q,\tilde{q}) p_{\tilde{q}M}(x),$$ (3.6)

where $p_{\tilde{q}M}$ is the probability of an actor belonging to threat class Q after running M boosting cycles; $c(q,\tilde{q})$ is the cost of mistakenly assigning an actor to threat class q when it belongs to class $\tilde{q}$.

Thus, the advantage of the proposed method of information security profile construction in social networking services is the automation of profile data processing procedures and the assignment of an actor to a given threat class. The advantage of the proposed classification approach is that it considers the cost of classification errors, which allows effective content monitoring of social networking services.

The method of building information profiles of actors proposed in the article allows to automate the procedures of early detection of threats to the information security of the state. On data of built profile by the information security system of the state is taken to attract actors to information operations in social networking services. The developed method differs from the known ones by applying modern methods of data mining, particularly methods of supervised machine learning and its generalization for use in various types of social networking services. Thus, building information

security profiles of actors increase the efficiency and speed of the information security system of the state in social networking services. However, in practice, this method requires verification and adaptation for a particular type of service depending on its actor profile attributes.

The input data for the experiment is a database of *Twitter* actors' accounts obtained within *TheFakeProject* [99], performed by a research team from the Institute of Informatics and Telematics of the Italian National Research Council (Italy) Structurally, the database consists of real user accounts and a set of fake accounts [100]. The set of real actors' profiles is created by aggregating the results of academic research projects *TheFakeProject* and #*elezioni2013* (University of Perugia and Sapienza University of Rome). In addition, many fake accounts were generated and purchased on the online microblogging network *Twitter* (http://fastfollowerz.com, http://intertwitter.com, http://twittertechnology.com). Three thousand fake accounts are stored in the respective database.

Given the fundamental differences in the concept of functioning of the microblogging network *Twitter* from other social networking services, the approach to the construction of actor information security profiles came to be adapted to take into account the following assumptions and limitations:

– *TheFakeProject's* database of *Twitter* microblogging user accounts is not representative and can only can solely from the initial stage of designing the information security profiles module of the state's information security system;

– the database does not synchronize actors' content publishing activity across time and topics, making it impossible to assign an actor to one of the threat classes based on content analysis of messages;

– the results of pre-processing the data do not introduce significant errors in the classification results.

A more detailed description of the experiment results and the limitations and assumptions adopted can be found in [101]. Finally, this paper will present the main results obtained and their description.

In order to evaluate the classification results, let's introduce the following metrics – accuracy, precision, recall, *F*-measure, and MCC (Matthew Correlation Coefficient). Then, based on the introduced metrics, the assumption of representativeness of the generated test set was verified, and the corresponding errors were estimated (**Table 3.3**). For this purpose, classification models were constructed using Random Forest, J48, and Bayesian Network machine learning algorithms, and classification results were evaluated using the metrics introduced in step 3.

Given the order of formation of the test set and the obtained errors of the introduced metrics, which at worst do not exceed 0.022, let's assume that the formed set is representative of the general population – the TheFakeProject database.

In order to select effective algorithms for binary classification, classification models are constructed based on the following algorithms: OneR, NaiveBayes, BayesNet, J48, RandomForest, DecisionTable, JRip, AdaBoost M1 (OneR), AdaBoost M1 (Naive Bayes). The selection results are unified by using the Weka data analysis system developed by the University of Waikato and the corresponding machine learning algorithms implemented in its libraries. The generalization ability of the

algorithms was evaluated using a cross-validation procedure with a partitioning parameter of 10. The structural diagram of the classification model construction sequence appears in **Fig. 3.9**.

● **Table 3.3** Inaccuracy of machine learning algorithms

Algorithm	Actor's roles set	Metrics				
		accuracy	precision	recall	F-measure	MCC
Random Forest	*TheFakeProject*	0.994	0.997	0.990	0.994	0.987
	Test set	0.994	0.994	0.994	0.994	0.987
	Inaccuracy	0.000	0.003	−0.004	0	0
J48	*TheFakeProject*	0.992	0.991	0.992	0.992	0.983
	Test set	0.987	0.987	0.987	0.987	0.974
	Inaccuracy	0.005	0.004	0.005	0.005	0.009
Bayesian Network	*TheFakeProject*	0.960	0.965	0.954	0.960	0.921
	Test set	0.971	0.972	0.971	0.971	0.943
	Inaccuracy	−0.011	−0.007	−0.017	−0.011	−0.022
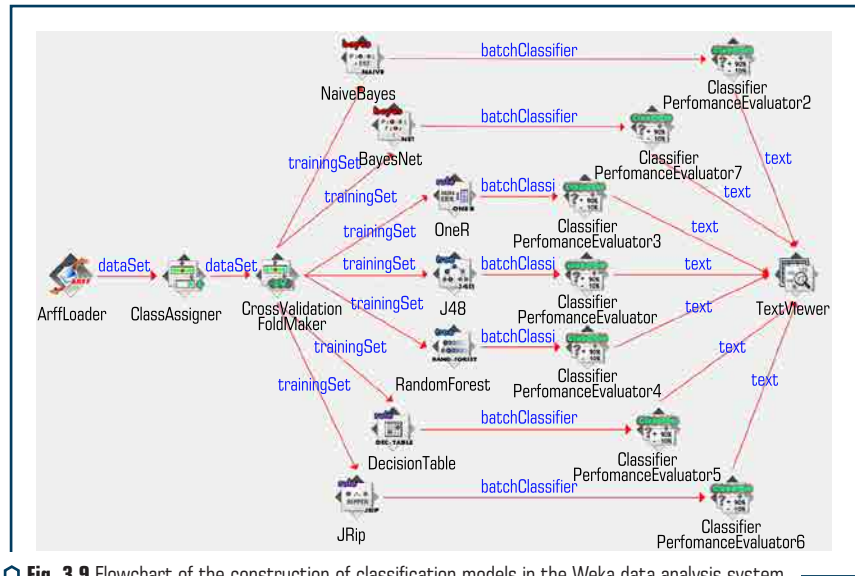
○ **Fig. 3.9** Flowchart of the construction of classification models in the Weka data analysis system

The test set was divided into the following classes: real active_real actor, passive_real actor, active_fake actor, and passive_fake actor. The division into such classes assumes that Metcalfe's

law is universal and can be applied not only to telecommunication networks but also to social networking services as networks of actors' social interactions. Based on this assumption, the usefulness of an actor as the subject of an information transaction is proportional to the square of the number of his/her friends. This effect is explained by the increase in the speed of content dissemination by an actor with the increase in the number of his/her friends and, consequently, the interest of the organizers of information operations in attracting him/her. Such actors are classified as active_real, otherwise as passive_real. A similar division is made for fake actor accounts.

For a more detailed analysis of the results of actor profile classification, three classification algorithms were selected from those that provided the highest values of the introduced evaluation metrics – J48, RandomForest, and JRip. The values of evaluation metrics for the selected machine learning algorithms obtained as a result of classification model building are presented in **Table 3.4**.

● **Table 3.4** Algorithm evaluation metrics by class

True class	Algorithm	accuracy	precision	recall	F-measure	MCC
PASSIVE_FAKE	J48	0.972	0.972	0.972	0.972	0.958
	RandomForest	0.991	0.982	0.991	0.986	0.979
	JRip	0.963	0.963	0.963	0.963	0.944
ACTIVE_FAKE	J48	1	0.957	1	0.978	0.975
	RandomForest	1	0.978	1	0.989	0.987
	JRip	0.956	0.956	0.956	0.956	0.948
PASSIVE_REAL	J48	0.976	0.984	0.976	0.980	0.967
	RandomForest	0.984	1	0.984	0.992	0.987
	JRip	0.976	0.969	0.976	0.973	0.954
ACTIVE_REAL	J48	0.968	1	0.968	0.984	0.982
	RandomForest	1	1	1	1	1
	JRip	0.935	0.967	0.935	0.951	0.946

Table 3.4 shows that the selected algorithms classify the active_real class as the best and the passive_fake class as the worst. The class active_fake is more precisely defined by J48 and JRip algorithms, while the class passive_real is defined by RandomForest and JRip algorithms. The RandomForest algorithm has an overall high accuracy in class allocation. The obtained results are similar to the results of academic research [31] and satisfy the performance requirements for threat detection subsystems in social networking services. The choice of a specific classification method to build actor information security profiles is appropriate depending on the specifics of the information operation in social networking services and the requirements for the accuracy and speed of the threat detection subsystem.

Thus, the effectiveness of the proposed approach to the construction of information security profiles of actors of social networking services to solve the problem of early detection of signs

of threats to information security of the state was proved experimentally. It established that the choice of the classification method is carried out the accuracy and speed requirements of the individual components of the information security system in the social networking services. The developed approach can be adapted for application in various types of social networking services, taking into account the peculiarities of their functioning. The use of the approach for the construction of information security profiles in social networking services will increase the overall efficiency of the system of information security of the state in social networking services.

3.4 INFORMATION-PSYCHOLOGICAL INFLUENCE ON ACTORS AND APPROACHES TO ITS EVALUATION

Social networking services create conditions for effective information operations using manipulative technologies in current conditions. For example, there is the low cost of content distribution in virtual communities and mobility of actor interaction processes; means for hiding sources of information actions; integrated use of various services and virtual communities; and hyperlinks to provide access to manipulative content directly from the service.

In this paper, manipulative features of information operations in social networking services are the presence of covert influence on actors in the content of virtual communities to alter their behaviour, goals, intentions or other psychological characteristics in the interest of the subject of power. Research [32] shows that the number of modern techniques for manipulating actors is growing due to new advances in psychology, linguistics, journalism, communication strategies, manipulative influence theory and other sciences. Let's summarize the following among the most effective technologies used in virtual communities in information operations.

The *«spiral of silence»* is a communication model proposed by E. Noel-Neumann, effective in social networking services and describes the specifics of the processes of expression and dissemination of public opinion. The essence of the model lies in actors' concealment of their civic position if it does not coincide with the majority point of view. In some cases, actors tend to agree with previously unacceptable statements.

The herd instinct of actors on social networking services is related to the collective behaviour of individuals and consists of a greater focus on publishing content or virtual communities with many comments, «likes», reposts, and participants. By such actions, attackers socialize a given content or virtual community, creating an illusion of active discussion, their importance and criticality for participants of the virtual community. Social bots are applied to implement this manipulation technique.

Opinion leaders in social networking services are actors or virtual communities of actors knowledgeable in a specific industry. They publish content with their evaluation, explanation and argumentation of events, and less active actors perceive it as an explanation of phenomena and facts. Paul Felix Lazarsfeld, the author of the Opinion Leader theory, argues that the perception of content occurs through two levels. First, the facts evaluate by opinion leaders through

the prism of their knowledge and skills. Then by applying interpersonal communication, they offer other groups of actors their vision of the situation, opinions, and conclusions. Thus, opinion leaders in social networking services indirectly influence the perception of facts by most participants in virtual communities. Using such manipulation technology, the subject of an information operation can disseminate specific ideas, imposing a desired point of view on events in the state and society.

Reference to an anonymous authority is limited to citing authoritative individuals such as politicians, academics, and clerics as a source of content. In addition, expert assessments, testimonies of participants in events, and documents are cited to increase the persuasiveness of the content. However, in such cases, the source of the facts is not identified, and no one is responsible for disseminating such content.

Emotional resonance in social networking services uses an emotional state for actors in virtual communities while simultaneously communicating content. This approach ensures the content is perceived at the level of emotion and disables logic and critical thinking mechanisms. It bases on the phenomenon of social induction, in which the emotional state of individual actors extends to other participants in virtual communities through empathy.

The distraction of the actors' attention aims at refocusing them from the primary content to the secondary content as a sensation. In this way, information noise is created in social networking services, hiding important events.

Myths or fakes are a technique for disseminating content on social media that contains distorted, disfigured facts about reality. This manipulation technique aims to ensure that actors perceive content as true without critically examining and verifying the facts. The dissemination of fakes is often combined with other techniques to achieve the desired effect by subjects of mind manipulation.

Neurolinguistic programming is used in social networking services to control actors' minds using specific linguistic constructs of content, images, pictures, and videos. The founders of neurolinguistic programming theory, R. Bendler and J. Grinder, investigated methods of influencing the personality to change its behavioural programs sustainably easily and quickly.

Thus, common signs of the use of manipulation in social networking services are:

— dubiousness of the facts presented, determined by the concealment of the sources and authors of information, insufficient argumentation, references to the opinion of the masses, and the presence of rhetorical questions;

— emotional colouring of content used to reflect the emotional state of its author and manifested in the oversaturation of content with figurative means, adjectives, and comparisons;

— tonality of content concerning some object or event, reflecting the value judgments of the actor and can be manifested in the use of images and emoticons;

— sensationalism of the content, which aims to attract the attention of actors through reference to the statements of scandalous persons, the use of words that increase anxiety;

— hidden (implicit) content is related to its underlying content, obtained as a result of mental activity based on the correlation of the actor's system of knowledge and values with linguistic units and constructions.

Identifying the signs of manipulative techniques used to conduct information operations in social networking services is a complex scientific task. Therefore, expert, programmatic, and combined approaches are used for their detection. The essence of expert detection is the involvement of experts or employees of special departments in the monitoring process to decide on the presence of manipulative techniques in content. The disadvantages of this approach are the subjectivity of expert assessments and the complexity of procedures for detecting hidden manipulations in content based on expert experience. On the other hand, it is reasonable to use software methods to detect threats in social networking services to manipulate public opinion. This approach helps to increase the speed of operation of the information security system of the state, which is based on modern content analysis technologies, intelligent content analysis and machine learning methods. The disadvantages of content analysis, produced using specialized software are the complexity of processes to clarify the purpose of the published content. It leads to uncertainty in the resulting estimate, mapping the judgments of a particular developer in the information software systems, namely, dictionaries databases and semantic search kernels, hidden nature of the linguistic structures of manipulation in the text content.

Furthermore, the application of content mining is limited by the complexity of extracting data from large data sets and the high cost in resource-limited environments. Combined methods are a combination of expert and software methods to compensate for their disadvantages. The advantage of using this group of methods is the reduction of subjectivity in assessing the content of social networking services, increasing the speed of decision-making in manipulative technologies, and improving the overall effectiveness of the virtual communities' information environment monitoring subsystem.

A methodology of identifying actors' manipulation of public opinion has been developed through textual content analysis and is based on modern data processing methods. The developed methodology uses content analysis and machine learning, does not contradict the research of V. Panchenko [102] and consists of the following.

Step 1. *Identify indications that the content is questionable*. The first step is to identify signs of the unreliability of the content of virtual communities of social networking services, reduced to the following:

– reference to a subjective point of view F_1 – a relative indicator of the application in the content of assessments of the facts by experts, scientists, and authoritative sources:

$$F_1 = \frac{R_d}{W}, \tag{3.7}$$

where R_d is the number of references detected; W is the total number of words;

– no argumentation F_2 – a relative indicator of using the linguistic constructions. Such constructions exclude the need to confirm and prove the truth of the content (e.g. obvious, indisputable fact, etc.):

$$F_2 = \frac{G_d}{W}, \tag{3.8}$$

where G_d is the number of linguistic constructions with denial of content verification;

– fraction of query sentences F_3 is the ratio of the number of query sentences S_{okl} to the total number of sentences S_z in the text content:

$$F_3 = \frac{S_{okl}}{S_z}, \tag{3.9}$$

numerical data F_4 – relative use of numerical data in the publication:

$$F_4 = \frac{B_z}{W}, \tag{3.10}$$

where B_z is the total number of numbers cited in the publication;

– F_5 is a relative indicator of the use of linguistic constructions that allow for different approaches to interpretation (e.g., *possible*, *probable*, *always*):

$$F_5 = \frac{F_z}{W}, \tag{3.11}$$

where F_z – the number of ambiguous statements.

Step 2. *Determining the emotional colouring of the content*. This step aims to determine the actor's moods or feelings about the studied objects or events in the textual content. The essence of the step is to detect the following features [104]:

– exclamation sentences F_6 – relative number of exclamation sentences S_d in the text content:

$$F_6 = \frac{S_d}{S_z}, \tag{3.12}$$

yelling F_7 indicates the presence of exclamations in textual content (e.g. *hey*, *aha*, *well-well* etc.):

$$F_7 = \frac{E_d}{W}, \tag{3.13}$$

where E_d is the number of detected exclamations in the publication;

– adverbs F_8 – relative number of adverbs A_d in the textual content used to compare and refocus the publication's reader on their emotions (e.g. *as if more*, *forever*, etc.):

$$F_8 = \frac{A_d}{A_z}, \tag{3.14}$$

where A_z is the total number of adverbs in the publication;

– emotional vocabulary F_9 – an indicator of the use of emotional lexemes in the publication (e.g. *unpunished*, *blockade*, *shameful*, etc.):

$$F_9 = \frac{V_d}{W}, \tag{3.15}$$

where V_d is the number of emotional lexemes.

Step 3. *Assessing the tone of the content*. The goal is to determine the actor's position on the studied objects or events. The task of assessing the tone of the content of virtual communities solves by machine learning and information retrieval.

This step reduces to assigning the publication's tone d_j, $j = \overline{1,n}$ to a pre-defined category c_j, $i = \overline{1,m}$ – negative, positive, neutral, etc.:

$$\left(d_j, c_i\right) \in D \times C, \tag{3.16}$$

where D is a collection of publications; C is a set of publication tonality classes.

Analysis of modern approaches to content tonality classification of social networking services showed that for the task of content tonality analysis, it is appropriate to use groups of methods given in **Table 3.5**.

● **Table 3.5** Groups of methods for detecting content tone of services

Name	Essence of the method	Advantages	Disadvantages
A rules-based approach	the tone of the content is determined by comparison with pre-defined rules	– high method accuracy with a complete rule base; – simple software implementation	– tone rules are created for a specific subject area; – low speed of evaluation
A supervised learning approach	approach is based on the use of tone dictionaries containing words with their tone values. The overall tonality of the content calculates by the selected method (e.g. arithmetic mean, learner classifier)	– ease of use in a given subject area; – ability to automate tone estimation procedures	approach is used within a specific subject area
A supervised learning approach	training a machine classifier on a collection of pre-selected content, which uses to analyze the tone of the content	– high accuracy and speed; – ability to automate procedures for assessing content tone; – availability of accuracy assessment tools; – and splitting content tone into a given number of classes	– approach is based on a training sample; – requires to develop of a classification model; – the criticality of the principle of training and validation sampling and test data
An unsupervised learning approach	approach is reduced to the task of determining the tone of the content without the intervention of the researcher making the connection between the objects	– easy to automate procedures for assessing the tone of content; – no training sample required; – no need for a priori information	– low accuracy; – high resource and cost; – low speed; – the undetermined number of classes in advance

Step 3 results in a defined textual content class Q_3 of the publication and a normalized numerical value according to the scale in **Table 3.6**.

● **Table 3.6** Example of a normalized pitch assessment scale

Tone class		Interval of the normalized grading scale
negative	**positive**	
strongly negative	strongly positive	1.00–0.70
moderately negative	moderately positive	0.71–0.50
neutral	neutral	0.51–0.40
moderately positive	moderately negative	0.41–0.20
strongly positive	strongly negative	0.21–0.00

Note 1. In the initial stages of the study, it is necessary to prioritize the tone class of the content, which is analyzed. The tone class depends on the object of the semantic core of the content.

Step 4. *Content sensationalism*. This step evaluates the textual content's ability to interest, impress, and attract the attention of the service actors. This step boils down to identifying the following attributes:

– attention-raising F_{10} – the relative use of words that attract the actor's attention, increasing anxiety (e.g., *murder*, *shock*, *separatism*):

$$F_{10} = \frac{U_d}{W},$$ (3.17)

where U_d – the number of attention-intensifying words identified;

– responsiveness F_{11} – an indicator of the use of words to create an atmosphere of the transience of events or phenomena, their urgency (e.g. *instantly*, *quickly*, *unexpectedly*):

$$F_{11} = \frac{O_d}{W},$$ (3.18)

where O_d – the number of identified words to indicate responsiveness.

Step 5. *Identifying the hidden content theme*. This step aims to identify the hidden theme of the message as a result of thematic modelling. In this paper, the topic of the content of social networking services means its main content that the author communicates to the reader.

Probabilistic topic modelling techniques are the most effective for automating the procedures for identifying the hidden subject of textual content. These techniques analyze a collection of documents and extract themes, connections between them, and their changes over time. The documents under study are considered as a set of unrelated words or Bags of words. For each publication in the social networking services d_i, the probabilities $P(t|d)$ of its belonging to the set of topics $t \in T$ calculates for each publication.

Table 3.7 presents state-of-the-art methods appropriate for identifying the hidden themes of social networking content.

● **Table 3.7** Methods for identifying hidden content topics

Name	Essence of the method	Advantages	Disadvantages
Probabilistic latent semantic indexing	functions based on an aspect model linking the latent parameters of the topic in the publication to each variable observed by the word or theme	– each publication relates to some topic with a given probability; – the method has statistical validity; – easy to implement	– the number of model parameters depends on the number of publications in the collection; – possible retraining of the model; – adding a new publication to the collection requires restructuring the model; – slow convergence on extensive collections of publications
Latent Dirichlet allocation	refers to generative models, which allow the construction of sentences according to the rules of a given language. A publication is considered a set of different topics a priori distributed by Dirichlet	– adequate for describing cluster structures; – simplifies the derivation of posterior probabilities of publications and their topics	– lack of linguistic justification for the method; – possible retraining of the model
Robust topic model	bases on the assertion that the use of a term in a document is explained by the topic, specific to the document (noise) or a commonly used term (background)	– removing background and noise from the publication that does not affect the topic of the publication; – better word appearance prediction criterion (perplexity) scores	the necessity to retain a considerable amount of additional model parameters

Note 2. For further estimation, the maximum probability value of the document belonging to one of the sets of content topics of interest of the social networking services for the research is used.

Step 6. *Calculate public opinion manipulation's information entropy in social networking services.* The relationship between particular attributes of public opinion manipulation in social networking services is discussed in steps 1–5 depicted as a hierarchy (**Fig. 3.10**).
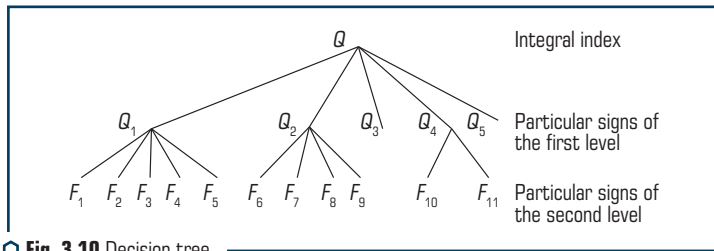
○ **Fig. 3.10** Decision tree

Let the manipulation of public opinion in the textual content manifest itself in k particular attributes. Denote the probability of occurrence of each of these attributes as P_v, $v = \overline{1, k}$.

Suppose N experiments are carried out to detect the signs of manipulation in the information flow of textual content. The number of signs of manipulation N_1, N_2, ..., N_k is set, and their sum equals N. Then, the total amount of identified information after all the experiments estimates by the expression:

$$I = -\left(N_1 \log_2 P_1 + N_2 \log_2 P_2 + ... + N_k \log_2 P_k\right) = -\sum_{v=1}^{k} N_v \log_2 P_v. \tag{3.19}$$

If the left and right-hand sides of equation (3.19) are divided by N, let's obtain the average amount of information about the presence of manipulation features in the textual content under study obtained over the experiment:

$$I_{avg} = \frac{I}{N} = -\sum_{v=1}^{k} \frac{N_v}{N} \log_2 P_v. \tag{3.20}$$

The ratio N_v/N represents the frequency of occurrence f_v of the corresponding sign of public opinion manipulation in the information flow of the textual content of virtual communities. When investigating many actors' publications, i.e. when N increases indefinitely, the frequencies of occurrence of features f_v will approach the corresponding probabilities P_v. Consider the problem of searching for a minimum amount of information whose limited value will determine the criterion of the presence of manipulative techniques for managing public opinion in the textual content of social networking services. Such a problem belongs to typical extreme problems with a condition because there is a function with k variables. The solution to this problem by the Lagrange method takes the form:

$$f_1 \equiv P_1; f_2 \equiv P_2; ... f_k \equiv P_k, \tag{3.21}$$

i.e., the least amount of average information about the presence of public opinion manipulation in the content of social networking services when the probability of occurrence of the v-th attribute P_v coincides with the marginal values of the corresponding frequencies f_v:

$$I_{avg\,min} = -\sum_{v=1}^{k} f_v \log_2 f_v. \tag{3.22}$$

The criterion for detecting manipulation in the textual content is then written as an inequality:

$$H = -\sum_{v=1}^{k} \sum_{l=1}^{g} Q_i^v \log_2 Q_i^v, \tag{3.23}$$

where H — the boundary value of information entropy (uncertainty); Q_i^v is the numerical value of the sign of manipulation of public opinion; $l = \overline{1,g}$ are the indices of second-level private signs of manipulation; $v = \overline{1,k}$ are the indices of first level particular signs of manipulation.

For ease of interpretation of the calculated values, let's introduce a normalized entropy value H_n:

$$H_n = \frac{H_{max} - H}{H_{max}}, \tag{3.24}$$

where H_{max} is the maximum value of entropy.

Thus, the content of the criterion of detecting manipulation of public opinion reduces to the evaluation of informational entropy of textual content of virtual communities. Informational entropy (3.24) decreases when the frequency of signs of manipulation of public opinion of actors in social networking services grows. Conversely, when the frequency of the signs of manipulation in the textual content of social networking services is low, information uncertainty grows. The qualitative scale for the threat assessment of actor manipulation of public opinion formed from the computational experiment, generalization and adaptation of approaches to information security threat assessment (**Table 3.8**).

● **Table 3.8** Adapted interval scale

Threat class	Interval values of the normalized entropy H_n
very high	0.00–0.20
high	0.21–0.49
significant	0.50–0.74
low	0.75–0.90
very low	0.91–1.00

Let's examine public opinion manipulation techniques in social networking services using the 2016 US presidential election campaign as an example. First, let's analyze the change in the pre-election ratings of US presidential candidates H. Clinton and D. Trump, obtained by *HuffPost Pollster* by targeting Internet users from January 1 to November 7, 2016.

Monitoring of *Twitter* microblogging showed that on June 10, 2016, there was a verbal altercation between the US presidential candidates. Following President Obama's support of H. Clinton, her rival once again published allegations of work-related correspondence from her home computer, violating federal law. The publications contained signs of manipulation – emotionality, negative tone, sensationalism. As a result of the incident, candidate support among social media actors changed, as shown in **Fig. 3.11, *a***. On September 16, 2016, as a result of years of controversy and conspiracy theories about the birthplace of incumbent US President B. Obama, D. Trump admitted that he was born in Hawaii. The debunking of the myth, which was actively supported by D. Trump's team and discussed by actors in social networking services, led to a negative impact on the candidate's rating (**Fig. 3.11, *b***). Also, on October 7, 2016, posts with disparaging remarks about women by D. Trump were distributed in the information space of social networking services. The analysis showed that the Facebook social network actively used opinion leaders to evaluate the event.

The posts were emotional with a strongly negative tone and aimed to discredit the candidate for President of the United States. After distributing such content, D. Trump's rating continued to fall, while that of his rival H. Clinton continued to rise (**Fig. 3.11, _c_**).
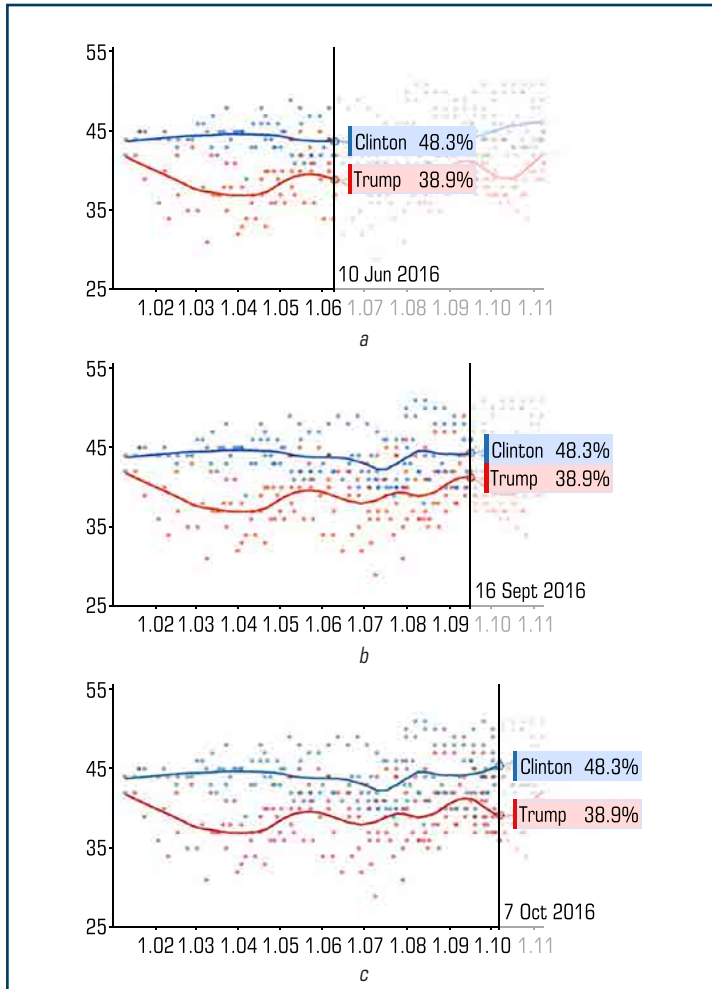

Fig. 3.11 Ranking of US presidential candidates:
_a_ – the candidates support among social networking services actors on June 10, 2016; _b_ – the candidates support among social networking services actors on September 16, 2016; _c_ – the candidates support among social networking services actors on October 7, 2016

A comprehensive analysis of the presidential election campaign in the USA showed active using the «spiral of silence» technique. As a result, the ratings of the candidates from different analytical agencies differed significantly from each other, and their teams announced their leaders as future winners in advance. It allowed voters to spread the idea of uncertainty and public uncertainty, and the absence of a predictable winner. Consequently, the analysis confirms the effectiveness of manipulative technology mechanisms used in social networking services to influence public opinion.

An experimental study of the proposed methodology for detecting manipulation of public opinion in social networking services has also been conducted. The textual content of the social network *VKontakte* and interaction methods with *VK API* service and *MS Visual Studio* integrated development environment served as a basis for the analysis. Textual content tone detection was implemented using the multinomial naive Bayesian method and latent topic detection using probabilistic latent semantic indexing. As a result, the following numerical values were obtained to calculate the entropy of particular attributes of public opinion manipulation in first-level social networking services, as shown in **Table 3.9**.

The visualization of the calculated data appears as a radar chart in **Fig. 3.12**.

● **Table 3.9** Calculated entropy values

	H_{a_1}	H_{a_2}	H_{a_3}	H_{a_4}	H_{a_5}
Value	0.30	0.40	0.34	0.52	0.50
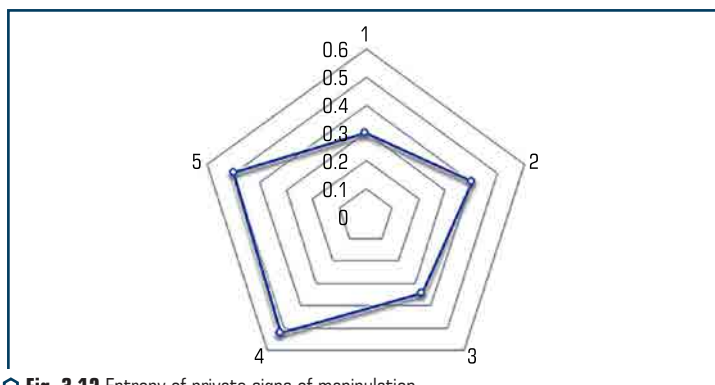
○ **Fig. 3.12** Entropy of private signs of manipulation

According to expressions (3.23), (3.24), the normalized entropy value for the data in **Table 3.9** is $H_n=0.67$. Thus, the textual content revealed significant manifestations of hidden themes and sensationalism, the presence of emotional vocabulary and the tone of the content. Consequently, the content under study contains a threat to information security of a significant level and therefore requires the adoption of measures to protect the information environment.

The considered methodology of detecting manipulation of public opinion based on intelligent analysis and accounting for information uncertainty in text content relies on total entropy, an integral indicator of the threat to information security of the state in the information space. However, the effectiveness of solving this problem would be improved by using conditional entropy «IF condition TO event», which is a promising direction for further scientific research. The model proposed in the publication considers the destructive information-psychological impact from content sources in social networking services and the increase of destructive influence due to processing and further dissemination by other actors of virtual communities. This approach makes it possible to increase the efficiency of detection of threats to the information security of the state in the information space of social networking services.

3.5 THE MODEL OF CONFLICTUAL INTERACTION OF CIVIC MOVEMENTS IN SOCIAL NETWORKING SERVICES

An example of the usage of social networking services for conducting information confrontation between the russian federation and the United States is the spread of disinformation containing a strategic anti-vaccination narrative. The research [35], which aim was to evaluate 2 million *Twitter* posts in 2014–2017, showed that russian trolls were more likely to write about vaccination than other social networking services actors. russian bots have been found to use anti-vaccine narratives as a problem issue to strengthen social discontent, undermine confidence in health care institutions and spread fear and split US citizens.

The consequence of such systematic information operations in the social networking services is the spread of the public movement that denies the effectiveness, safety, and legitimacy of vaccination, in particular, the mass one. The sceptical attitude towards vaccination includes both a complete denial of vaccinations and particular vaccines, which causes a change in the timing and of immunization schedules of the recommended by medical establishments. As a result of the increased anti-vaccine movement in Ukraine and the world in general, the number of patients and fatal cases has increased significantly. On the other hand, this has led to the formation of virtual communities that are opposed to the anti-vaccine movement. The latter is aimed at counteracting the movement of anti-vaccines and is in conflict with its supporters.

A promising area of research is the study of peculiarities of information confrontation of virtual communities aiming to reduce the level of threat to the national security of the state by counteracting destructive content in social networking services. Therefore, there is an objective contradiction between ensuring the sustainable development of the social networking services information space in the context of globalization and the free circulation of information and lack of effective methodological tools for the investigation of the conflict interaction of virtual communities in order to ensure the information security of the state.

To identify the signs of conflict of virtual community actors in the social networking services, let's determine the interests of the conflicting parties. The essence of the narrative spread

by pro-vaccination virtual communities in the social networking services information can be the following: a significant reduction of the risk of catching the disease due to conducting the appropriate vaccinations. According to *the World Health Organization*, immunization prevents from 2 to 3 million deaths each year. It is one of the most effective types of investments in health care in terms of their value [105–107].

The interests of the virtual communities that are adherents of the anti-vaccine movement are manifested in the social networking services by spreading content with the following narratives:

1) denying the role of vaccination as the factor that reduces the sickness rate;

2) the denial of the necessity of vaccination at present. It is claimed that mass vaccination against all or most of the diseases is inappropriate, since modern treatments for the diseases, which vaccination is carried out from, are effective enough, and the frequency of these diseases themselves is pretty low.

Thus, the essence of the conflict lies in the fact that in real life, social networking services' actors who oppose vaccination as a result of refusing vaccinations become vulnerable to the disease and also become a threat to those who have been vaccinated. At the same time, the conflict that takes place in the social networking services information space influences public opinion in real life and encourages citizens to take certain actions and creates the background for the emergence of threats to the information security and national security of the state as a whole. Moreover, the considered conflict interaction of virtual communities can be characterized as antagonistic – features intransigence and hostility between groups of actors and manifests in conflict on an ideological basis.

The choice of the type of differential equation of the dynamics of information confrontation of virtual communities is an important issue from the point of view of the study of conflict interaction in the social networking services information space. Let's choose the function of limited growth to formalize the conflict interaction of virtual community actors, which combines accelerated growth in the initial phase and accelerated deceleration in the final phase of antagonistic conflict. Such kind of differential equation includes control parameters [108]. Therefore, let's choose the general equation of limited growth in the form of a second-order nonlinear differential equation as the equations of conflict dynamics:

$$a_2 w(t) \frac{d^2 w(t)}{dt^2} + \left(1 + a_1 w(t)\right) \frac{dw(t)}{dt} + \left(a_0 w(t) - \beta^+\right) \vartheta w^\theta(t) = 0, \tag{3.25}$$

where $w(t)$ is the studied indicator of conflict interaction; a_2, a_1, a_0 are parameters that represent vectors of latent control; ϑ, θ are parameters of multiplication of variables.

There is some characteristic value W for solving the differential growth equation $w(t)$, for which all components of expression (3.25) become zero at:

$$\frac{d^2 w(t)}{dt^2} \approx 0; \ \frac{dw(t)}{dt} \approx 0; \ a_0 w(t) - \beta^+ \approx 0. \tag{3.26}$$

The value $W = \beta^+/a_0$ is called the threshold of the function of limited growth, to which the values of the state variables at large values of the time interval direct asymptotically. Thus W is a characteristic parameter of the function of limited growth that physically determines some limit value that studied value can reach. From general equation (3.25) it is possible to obtain partial cases, among which let's emphasize those that have a threshold character (**Table 3.10**).

● **Table 3.10** Partial cases of the general equation of limited growth

No.	Name of the equation of limited growth	Conditions	The form of the equation of limited growth
1	the second order constrained growth equation	–	$a_2 ww'' + (1 + a_1 w)w' + (a_0 w - \beta^+)w = 0$
2	first order restricted growth equation	$a_2 = 0$	$(1 + a_1 w)w' + (a_0 w - \beta^+)w = 0$
3	first order constrained growth equation (Verhulst logistic equation)	$a_2 = 0,$ $a_1 = 0$	$w' + (a_0 w - \beta^+)w = 0$

All growth equations are characterized by a common element $(a_0 w - \beta^+)$ used to determine the threshold. Since the logistic equation is a particular case of the differential growth equation (3.25), the equilibrium region of the growth equation is valid for it. Although for the implementation of component models any equations in **Table 3.10** can be used, the most constructive approach is the application of the first order constrained growth equation:

$$(1 + a_1 w(t))\frac{dw(t)}{dt} + (a_0 w(t) - \beta^+)w(t) = 0.$$

The threshold of the function of limited growth W is considered as a parametrically dependent value. The solution of this differential equation is the function of growth of the investigated value, which is a description of the conflict of virtual communities in the social networking services.

Let's present separate layers of the equation of the model of conflict dynamics based on the limited growth of the first order [94, 108]. The first layer of the model describes the dynamics of the number of two virtual communities – supporters $x(t)$ and $y(t)$ opponents of vaccination who are in antagonistic conflict:

$$\begin{cases} (1 + ax(t))\dfrac{dx(t)}{dt} + \psi\left(\dfrac{x(t)}{X} - 1\right)x(t) = 0; \\ \dots \\ (1 + bx(t))\dfrac{dy(t)}{dt} + \varphi\left(\dfrac{y(t)}{Y} - 1\right)y(t) = 0, \end{cases} \qquad (3.27)$$

where a, b are the parameters that prevent the increase in the number of actors of the corresponding virtual communities in the social networking services; ψ, φ are exponential growth

indicators contributing to the growth of the number of actors; X, Y are limit values of the number of actors of opposing virtual communities.

For curves that describe limited growth, characteristic parameters $X = \psi/a$ and $Y = \varphi/b$ that limit the growth in the number of actors in the respective virtual communities are important. The conflict of actors is manifested in the fact that their total number is considered to be constant $x(t) + y(t) = N(t) = \text{Const}$, and each virtual community tries to increase its number.

The second layer of the model formalizes the growth of resources $r(t)$ and $s(t)$ — corresponding benefits of virtual communities:

$$\begin{cases} \left(1 + cr(t)\right)\dfrac{dr(t)}{dt} + \alpha\left(\dfrac{r(t)}{R} - 1\right)r(t) = 0; \\ \dots \\ \left(1 + ds(t)\right)\dfrac{ds(t)}{dt} + \beta\left(\dfrac{s(t)}{S} - 1\right)s(t) = 0, \end{cases} \qquad (3.28)$$

where c, d are parameters that adversely affect the level of winnings resulting from information confrontation in the social networking services; α, β are exponential growth rates of gain; R, S are thresholds for the winnings of virtual communities.

For curves, the characteristic parameter that limits the gain growth $R = \alpha/c$, $S = \beta/d$ is important. In this case, the limit values of the resources $r(t)$ and $s(t)$ depend on the threshold values of the number of actors of virtual communities in social networking services $x(t)$ and $y(t)$. At the same time the amount of winnings is not constant, which is connected with the non-deterministic behaviour of the actors in the social networking services information space.

The third layer of the model characterizes the dynamics of resource expenditures for information confrontation in social networking services:

$$\begin{cases} \left(1 + gp(t)\right)\dfrac{dp(t)}{dt} + \zeta\left(\dfrac{p(t)}{R} - 1\right)p(t) = 0; \\ \dots \\ \left(1 + hq(t)\right)\dfrac{dq(t)}{dt} + \xi\left(\dfrac{q(t)}{S} - 1\right)q(t) = 0, \end{cases} \qquad (3.29)$$

where g, h are the parameters that negatively affect the cost level; ζ, ξ is intensity of expenditures for conducting operations (exponential growth rates); P, Q is the maximum amount of resources allocated for conducting the conflict $P = \zeta/g$, $Q = \xi/h$. The amount of resources spent on information warfare is also variable.

Resource limits $r(t)$ and $s(t)$ depend on the thresholds of the number of actors $x(t)$ and $y(t)$. In simple cases, let's restrict ourselves to a linear dependence in the form $R = \lambda X$, $S = \mu Y$. At the

same time, resource limit values depend on the threshold's values of the number of virtual communities' actors involved in the conflict $S=f(Y)$, $R=f(X)$, $P=f(X)$, $Q=f(Y)$.

The nature of communication depends on the investigated aspect of the subject area. In simple cases, it is possible to limit ourselves to a linear dependence of the form $S=\mu Y$, $R=\lambda X$ that sets the scale of the output function. For linear dependence, there may occur difficulties connected with the decrease of the value of the function $y=f(t, u, v)$ in time. Let's assume that as the number of actors of the virtual community in a state of conflict decreases, then the winnings and resources of this community in the management of information warfare also decreases. Suppose that these quantities will vary in a complex way, which is related to the inverted S-shaped nature of the function $y=f(t, u, v)$ and the requirement to fulfill the condition $x+y=z$. However, a non-inverted S-function must be used to describe the benefits and expenditure of resources. To resolve this discrepancy, let's use the following technique.

As a function of movement of gained resources and expense of resources let's use the functions of the limited growth with a variable value of a threshold, where the current values of the function of the original are used as the threshold, i.e. $S=f(y)$, $R=f(x)$, $P=f(x)$, $Q=f(y)$. Such dependence of threshold values is algorithmic and can be considered as a way of parametric control of movement of resources. Such functions can be convex in nature, which distinguishes them from the classic S-shaped features that have a monotonous growth pattern. Thereby, the constrained growth functions with a variable threshold value describe the relationship with the inverse S-function more adequately.

Let's write the layers (3.27), (3.28) in the form of recurrent formulas similarly to the expression (3.29). The results of a study [109] showed that a rigid stance against vaccinations is supported only by a small number of parents, whereas various forms of «vaccine scepticism» and uncertainty about the need for vaccination are more widely spread. Less than 2 % of parents fully reject vaccination, while selective or late vaccination is practiced by 2 % to 27 % of parents. «Vaccine hesitant» is from 20 % to 30 % of parents [109]. To conduct computational experiment, let's consider the situation where the number of actors who oppose vaccination has reached the critical mark of 30 % – the value that precedes the start of the epidemic. To reduce the threat of the epidemic, let's consider the following scenario: as a result of preventive work, in particular in the social networking services information space, the number of vaccine opponents is reduced to 5 %, and the number of vaccination supporters is increased to 95 % (**Fig. 3.13**).

The speed of change depends on the values of the control parameters *a* and *b* which are determined by the level of unacceptance by the actors of the relevant virtual communities of the narrative concerning the importance of early vaccination in order to prevent epidemics. It is possible to reduce the value of these parameters by transferring information to the virtual anti-vaccine community in an accessible form in order to influence their public opinion. The resulting values of the number of actors who are supporters and opponents of vaccination will be used as the current value of the conflict interaction function.

Fig. 3.14 shows the curves that describe the change in the normalized values of the information resource in the social networking services and the costs of maintaining information warfare

campaigns of the virtual community of vaccination supporters as a result of the redistribution of actors between the virtual communities (**Fig. 3.14**).
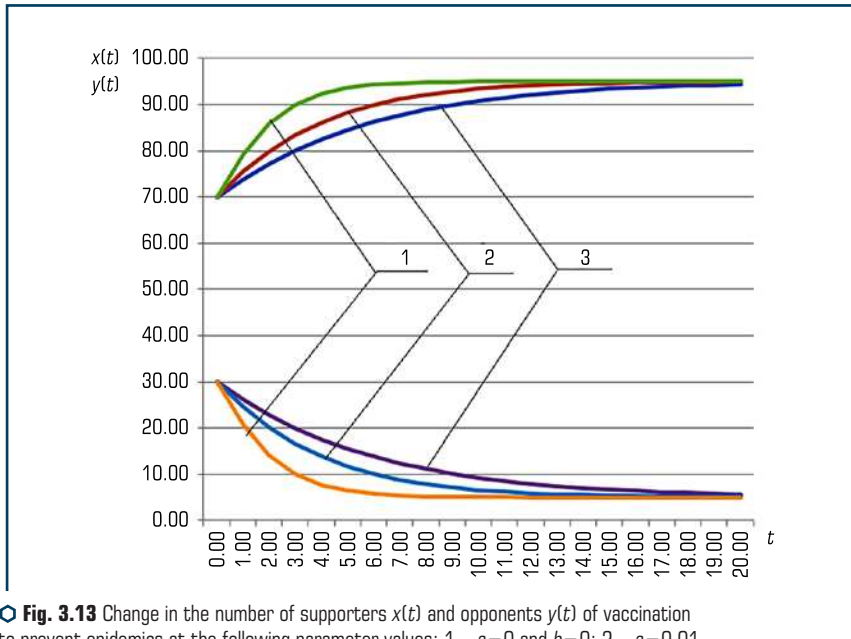

○ **Fig. 3.13** Change in the number of supporters $x(t)$ and opponents $y(t)$ of vaccination to prevent epidemics at the following parameter values: $1 - a=0$ and $b=0$; $2 - a=0.01$ and $b=0.01$; $3 - a=0.02$ and $b=0.02$

Fig. 3.14 shows that the value of the normalized benefit of the virtual community compared to the normalized value of the cost is 2 times higher. So, every 1 conventional unit the resource spent on information confrontation gives 2 conventional units gain in the context of the information resource in 20 days.

Fig. 3.15 shows the dynamics of the normalized values of the information resource in the social networking services and the costs of information warfare of the virtual community of the opponents of vaccination after the redistribution of actors between virtual communities in a state of conflict.

Dependencies are described by convex curves, which are explained by the use of variable growth functions with variable thresholds. Also **Fig. 3.15** shows that after 20 days each conventional unit of the resources spent on information warfare will give 0.5 of conventional units of gain in the virtual community information space, that is, resource expenditures are more than double the winning value. The extended results of the research are presented in article [110]. Such information confrontation between virtual communities is ineffective and will eventually lead to a further reduction in the number of opponents of the vaccination and significant losses of resources available for conflict interaction.
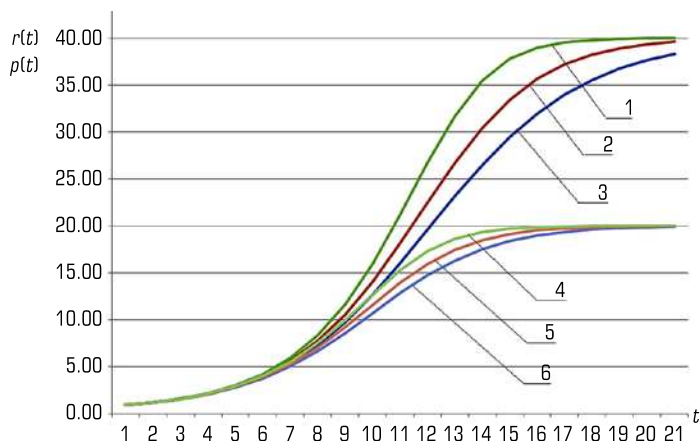
○ **Fig. 3.14** Dynamics of benefit $r(t)$ at parameter values (curves 1–3) at $c = \{0; 0.01; 0.02\}$ and resource costs $p(t)$ (curves 4–6) for the virtual community of vaccination supporters at parameter values $g = \{0; 0.01; 0.02\}$
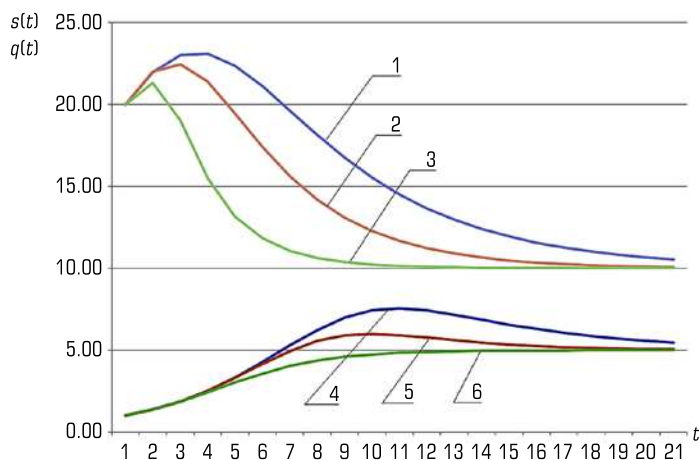

○ **Fig. 3.15** Dynamics of resource expenditures $q(t)$ (curves 1–3) for $h = \{0; 0.02; 0.01; 0\}$ and benefit $s(t)$ (curves 4–6) $d = \{0; 0.02; 0.01; 0\}$ for the virtual community of vaccination advocates

3.6 THE CONCEPTUAL MODEL FOR MANAGED SELF-ORGANIZATION IN SOCIAL NETWORKING SERVICES

Modern synergetic control theory of nonlinear multidimensional and multi-connected dynamic systems for controllability of self-organization processes in various systems, such as technical, social, economic and others, rely on the analytical construction of nonlinear aggregated regulators [111].

Synthesis of control laws for targeted self-organization of interaction in social networking services based on the method of analytical construction of nonlinear aggregated regulators, reveals the essence of the developed concept. Let's present the developed concept of synergetic management of interaction in social networking services in the form of an appropriate conceptual model.

This model allows to take into account the peculiarities of social networking services, social communication processes in virtual communities and the requirements of the feasibility of hidden control action [112]. The conceptual model components are formalized as a set of concepts — a set of meanings of concepts (**Table 3.11**).

The concepts mentioned in **Table 3.11** have been used to build a systemic triad model of interaction management processes in social networking services, consisting of two hierarchical levels (**Fig. 3.16**).

● **Table 3.11** Characteristics of the conceptual model

| The set of concepts	The variables of concepts	The essence of concepts
$D = \{D_\alpha\}$	$\{D_\alpha\}$	Threats to information security of the state targeting actors of virtual communities in social networking services
$K = \{K_\beta\}$	$\{x_i(t), y_j(t)\}$	Functions of actor interaction processes in social networking services
$Z = \{Z_\lambda\}$	$\{Z_\lambda\}$	Parameters of the external information space of social networking services
$I = \{I_\kappa\}$	$\{I_\kappa\}$	The parameters of the internal information space of social networking services
$\Psi = \{\psi_\upsilon\}$	$\{\psi_\upsilon(t)\}$	The preferred evolutionary trajectory of the virtual community of actors
$U = \{u_\gamma\}$	$\{u_\gamma(t)\}$	Synergetic management of actors' interaction in social networking services
$S_{real}^{w} = \{S_\tau\}$	$\{x_i^0, y_j^0\}$	The current state of information security of the state in which social networking services operates
$S_{accept}^{v} = \{S_\varphi\}$	$\{x_{i\upsilon}, y_{j\upsilon}\}$	The expected state of information security of the state, which is reached with the given values of the actor interaction function in the social networking services
$F = \{F_\varsigma\}$	$\{F_\varsigma\}$	Information influences on actors to manage the processes of interaction in social networking services
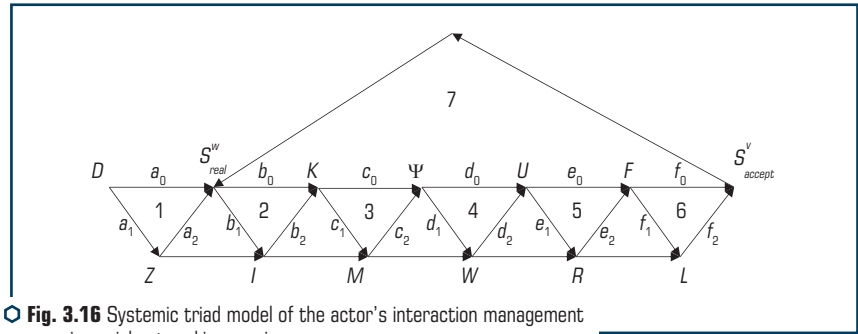
○ **Fig. 3.16** Systemic triad model of the actor's interaction management process in social networking services

Each hierarchy level appears as a triad — a graph with three vertices. Each triad is a set of objects (vertices) equivalent to each other and connected by relations (edges). Thus, the triads formed due to the study results in **Table 3.12**.

Thus, the proposed concept of synergetic management of actors' interaction in social networking services forms the basis for creating a multi-agent system model. In this case, objects and subsystems, which take part in opportunistic management of the actors' behaviour in virtual communities of social networking services, are considered agents. Using a systematic approach allowed to identify components of the multi-agent system model presented in **Fig. 3.17**: sources of threats to information security of the state; mass information tools; actors; social networking services; module for monitoring the information space of social networking services; synergetic management synthesis module; information security expert; module for combating threats to information security of the state in social networking services.
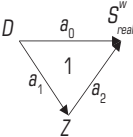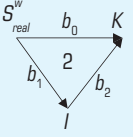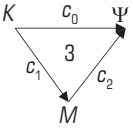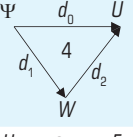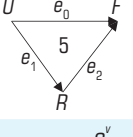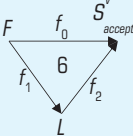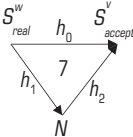
The first component of the developed model is the sources of threats to information security of the state, which form a multitude and negatively influence the following components — mass media, actors and social networking services. The result of such threats to mass media and social networking services is changing both in the external and internal information space of social networking services.

As a result, the parameters of interaction between actors change, leading to chaotic dynamics in social networking services and the transition of virtual community to unmanageable state in virtual space and real life.

The fifth component of the system model is an information space monitoring module, which detects threats to the information security of the state based on an analysis of the internal information space of social networking services and peculiarities of actor interaction processes. After that, an information security expert of the state selects an order parameter, and the synergetic control synthesis module produces the appropriate controlling influence on actors in social networking services. The eighth component of the model is the module for counteracting threats in social networking services. It provides practical recommendations for implementing synergetic

management as information influences and starts the processes of actors' self-organization and transition of the service to a given steady-state of information security of the state.

● **Table 3.12** Requirements for system model triads

| Triad number	Relationship between the vertices	Essence of the triad
1 — D, a_0, S_{real}^w, a_1, a_2, Z	$a_0 : D \rightarrow S_{real}^w$; $a_1 : D \rightarrow Z$; $a_2 : Z \rightarrow S_{real}^w$	describes the current state of information security of the state in social networking services. The set of threats D is reflected in the set of possible current levels of information security of the state in social networking services and simultaneously affects the external information space Z of the set of services
2 — S_{real}^w, b_0, K, b_1, b_2, I	$b_0 : S_{real}^w \rightarrow K$; $b_1 : S_{real}^w \rightarrow I$; $b_0 : I \rightarrow K$	depending on the current level of information security of the state S_{real}^w established in the social networking services, the parameters of actors' interaction K processes change. The set of parameters I characterizing the internal information space of social networking services is formed as a consequence of mapping S_{real}^w and, in its turn, influences the set of parameters K
3 — K, c_0, Ψ, c_1, c_2, M	$c_0 : K \rightarrow \Psi$; $c_1 : K \rightarrow M$; $c_2 : M \rightarrow \Psi$	transmits the set K to the set of functions of the order parameter Ψ. Using the set K, the choice of the manageable aspect of actor interaction and the type of the expected attractor based on the results of information monitoring, formulated set of requirements M to the information security of the state is carried out
4 — Ψ, d_0, U, d_1, d_2, W	$d_0 : \Psi \rightarrow U$; $d_1 : \Psi \rightarrow W$; $d_2 : W \rightarrow U$	allows synthesizing synergetic control U based on a set of order parameters Ψ. The set Ψ forms a set of constraints W on the set U, the fulfillment of which ensures the stability of the achieved given state of information security of the state in social networking services
5 — U, e_0, F, e_1, e_2, R	$e_0 : U \rightarrow F$; $e_1 : U \rightarrow R$; $e_2 : R \rightarrow F$	implements the mapping of pre-produced synergetic control U to the set of information impacts on actors F. The implementation of the synthesised control U set taking into account the set of available system resources of the information security system of the state R
6 — F, f_0, S_{accept}^v, f_1, f_2, L	$f_0 : F \rightarrow S_{accept}^v$; $f_1 : F \rightarrow L$; $f_2 : L \rightarrow S_{accept}^v$	realizes the transition from a set of information influences F to an expected state of information security of the state in social networking services S_{accept}^v through the emergence of an expected synergy effect from a set of L
7 — S_{real}^w, h_0, S_{accept}^v, h_1, h_2, N	$h_0 : S_{real}^v \rightarrow S_{accept}^v$; $h_1 : S_{real}^v \rightarrow N$; $h_2 : N \rightarrow S_{accept}^v$	transits virtual communities of actors in social networking services from the set of current states of information security S_{real}^v to the set of given steady states of information security S_{accept}^v through the set of actors' actions in the virtual communities N
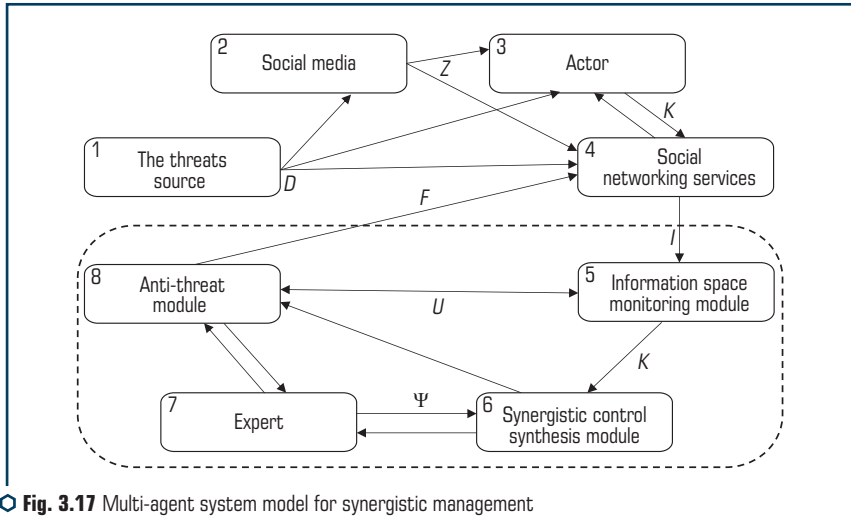
○ **Fig. 3.17** Multi-agent system model for synergistic management of actor interaction in social networking services

Publications [112, 113] synthesized models of synergetic management of actor interaction in the social networking services, and publication [113] developed a model of decision support system to identify signs of national information security threats in social networking services and assess their level. However, there are no practical recommendations for choosing a specific system of nonlinear differential equations and the model of synergetic management; therefore, the decision is entrusted to experts who work with the decision support system. Involving experts in the work of the decision support system at the stage of countering threats in terms of choosing a model of synergetic management has a number of disadvantages, in particular: increasing the level of subjectivity; inertia of the decision-making process; high level of requirements for expert knowledge, etc. Reducing the negative impact of such factors is achieved through the use of decision-making methods without expert involvement.

Due to controversial requirements when choosing a model of synergetic management, ambiguity in assessing the level of national information security threats in social networking services, the difficulty of determining priorities, lack of generally accepted rules for choosing a model for formalizing the interaction of actors in virtual communities and synergetic management, decision-making procedures become more complex. Therefore, an effective way to eliminate them is to use the mathematical apparatus of fuzzy sets [114]. It is promising to develop a model of a decision support system based on a fuzzy inference. Such systems combine the basic statements of the theory of fuzzy sets and allow solving issues related to decision-making on weakly structured and complexly formalized study objects. Thus, the development of the decision support system model for managing the actors' interaction in social networking services will ensure the effective transition

of the virtual community to a given state of national information security, which will additionally update the chosen direction of current research.

To counter national information security threats in social networking services effectively, at first it is necessary to define a mathematical model for formalizing the interaction of actors, and then directly choose a model of synergetic management, which will make an artificially controlled transition to a given state of interaction parameters in the information space of services. The choice should be made in accordance with the characteristics of the information space of social networking services, which describe the features of threat activities related to information security of the state. Therefore, the procedure of selecting models of synergetic management by experts is described by the decision tree, which is presented in **Fig. 3.18**.
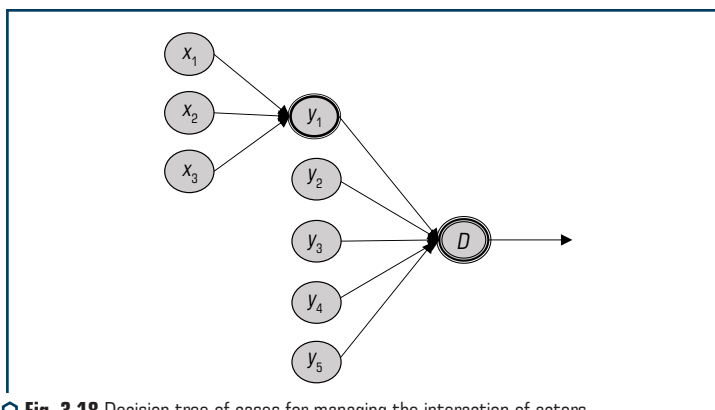

○ **Fig. 3.18** Decision tree of cases for managing the interaction of actors

The indicators that determine the approach to the formalization of the actors' interaction in the form of a system of nonlinear differential equations and directly synergetic management models are the following: x_1 – the confrontation level of actors in virtual communities; x_2 – the engagement of external information resources for threat activities in social networking services; x_3 – the influence level of the narrative spread by intruders on the formation of public opinion on certain issues among actors; y_1 – recommended model of actors' interaction in social networking services; y_2 – the level of actors' demand for destructive content; y_3 – the supply level of destructive content in the information space of social networking services; y_4 – the duration of the information campaign in services information space; y_5 – the intensity of changes in the operational situation in the information space of social networking services.

The initial variable of the system is D – the decision on the choice of the synergetic management model, the models of which are developed in publications [83, 85, 86]. Let's present the interdependence of the chosen indicators for the qualitative characteristic of actors' interaction as a system of relations:

$$y_1 = f(x_1, x_2, x_3); \qquad\qquad (3.30)$$

$$D = f(y_1, y_2, y_3, y_4, y_5). \qquad\qquad (3.31)$$

The input and output variables of the fuzzy inference system acquire values defined by their universal sets and are estimated by fuzzy terms according to **Table 3.13**.

● **Table 3.13** Linguistic terms of variable systems of fuzzy inference

Fuzzy variable	Universal set of fuzzy variables	Linguistic variable
x_1		Low (*L*); Medium (*M*); High Medium (*HM*); High (*H*)
x_2		Low (*L*); Medium (*M*); High Medium (*HM*); High (*H*)
x_3		Low (*L*); Medium (*M*); High Medium (*HM*); High (*H*)
y_1		Predator – prey interaction model (*IM₁*); Mono model (*IM₂*)
y_2	[0;1]	Low (*L*); Medium (*M*); High Medium (*HM*); High (*H*)
y_3		Low (*L*); Medium (*M*); High Medium (*HM*); High (*H*)
y_4		Small (*S*); Medium (*M*); Large (*L*); XLarge (*XL*)
y_5		Low (*L*); Medium (*M*); High Medium (*HM*); High (*H*)
D		Model of synergetic demand management (*M₁*); model of synergetic maintenance of a given level of demand (*M₂*); model of forming a stable virtual community (*M₃*)

Fuzzy production rules presented in publication [115]. In turn, the Sugeno algorithm is characterized by adaptation to solving identification problems. Therefore, to implement a fuzzy inference system to select a model of synergistic management of actors' interaction in the social networking services, let's use the Mamdani algorithm. The essence of Mamdani algorithm for the decision-making problem on the choice of synergetic management model follows such steps [114]:

Step 1. *Fuzzyfication of the input variables* of the system where $i = \overline{1,3}$ and the output variable is $Y = \{y_i\}$. To do this, let's use an *S*-shaped increasing function $\mu_1(x_1)$, two models of a *U*-shaped function $\mu_2(x_i), \mu_3(x_i)$ and an *S*-shaped descending one $\mu_4(x_i)$ [8]. Fuzzyfication of the remaining input and output linguistic variables of the decision support system are performed similarly.

Step 2. *The aggregation of subconditions in fuzzy* production *rules* [115] is reduced to finding the truth degree for the conditions in each rule of the pre-formed rule base through logical operations. In this case, operations AND or OR are replaced to the conjunction $(\wedge)$ or disjunction $(\vee)$ respectively through maximization operations or minimization ones.

Step 3. *The activation of the subconclusion in the knowledge base rules*, which is performed using the min-activation method according to which:

$$\mu_j(x_i) = \min\{n_m, \mu_j(x_i)\}, \tag{3.32}$$

where n_m determines the truth of a particular rule of the knowledge base. However, inactive knowledge base rules are not taken into account in order to reduce data processing time.

Step 4. *Accumulation of the conclusions of fuzzy production rules* is carried out for association of those fuzzy sets which correspond to terms of subconclusions concerning the same initial variables:

$$\mu(y_i) = \left\{\mu_{y_1}(x_1, x_2, x_3)\right\}. \tag{3.33}$$

Step 5. *Defuzzification of the output variable* y_1 is performed according to the plane center method for which:

$$\int_{min}^{u} \mu(x_j)dx = \int_{u}^{max} \mu(x_j)dx. \tag{3.34}$$

The above algorithm describes the fuzzy inference procedure for the functional dependence (3.31). To implement the functional relationship in the decision support system (3.30), it is necessary to perform similar steps 1–5 for the input variables $Y = \{y_k\}$, $k = \overline{1,5}$ and the output variable $D = \{d\}$.

Let's study the developed model of the decision support system for managing the interaction of actors in the social networking services using the *Fuzzy Logic* environment of the *MatLab* application package. To this, consider the example of an information operation in the social networking services, aimed at forming a negative public opinion in society about Ukraine's accession to *NATO*. The input data for the decision support system for managing the interaction of actors in the social networking services are expert assessments of the Information Protection and Cybersecurity Department of Korolov Zhytomyr Military Institute (**Table 3.14**), obtained on the basis of public opinion data in Ukraine on Euro-Atlantic integration in 2019 and summarized information about the information campaigns in the social networking services, aimed at the freedom of choice of citizens.

The expected forms of the first step results of the Mamdani algorithm for the linguistic variable x_1 are given in **Fig. 3.19**.

The results of defuzzification of the initial variable d of the decision support system are shown in **Fig. 3.20**.

To visualize the dependence of the output variable d on the values of the input y_2 and y_5 constructed a three-dimensional surface (**Fig. 3.21**).

● **Table 3.14** Set of input data for the decision support system

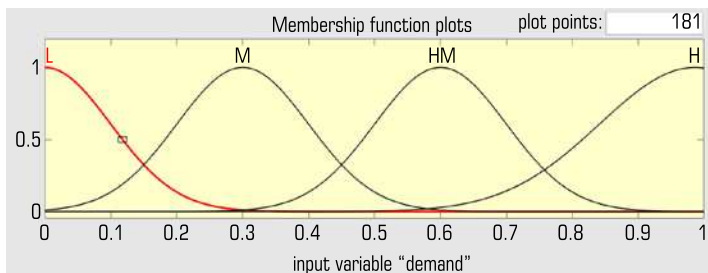|	x_1	x_2	x_3	y_2	y_3	y_4	y_5
Meaning	0.6	0.8	0.6	0.2	0.7	0.3	0.5

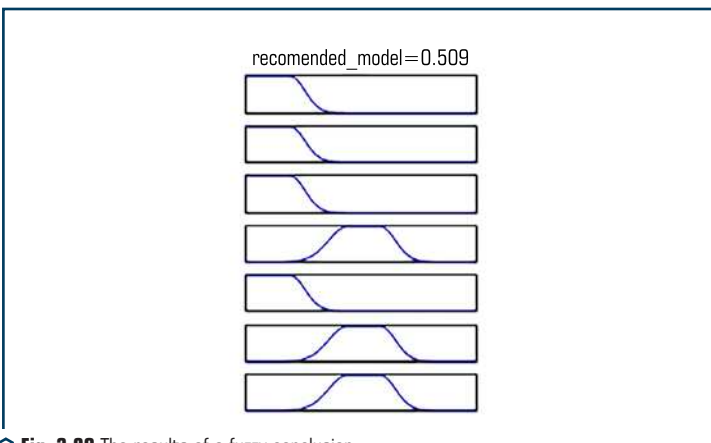**Fig. 3.19** The membership functions graphs of a linguistic variable x_1

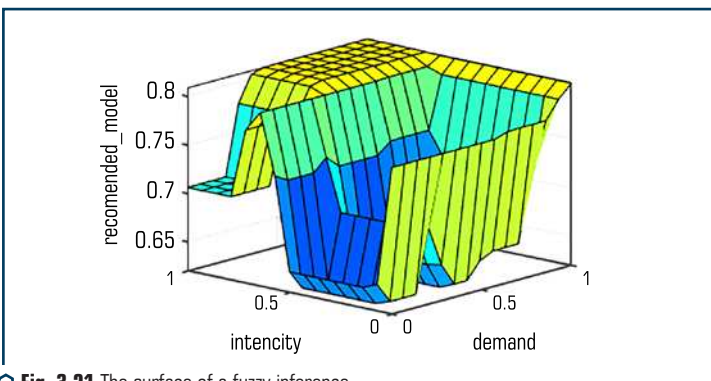**Fig. 3.20** The results of a fuzzy conclusion

Fig. 3.21 The surface of a fuzzy inference

The given surface in **Fig. 3.21** can be used to further improve the decision-making process in order to increase their adequacy for different values of the threat level to national information security in the social networking services.

Therefore, to counteract the considered threat to information security in the social networking services, it is necessary to apply the M_2 model of synergistic support of a given demand level for certain content [112, 113]. To do this, it is necessary to publish the number of posts specified in accordance with this model in the social networking services information space.

As a result of the research, for the first time the model of a decision support system for managing the actors' interaction in the social networking services was introduced, which is based on a fuzzy logic conclusion. This approach provided an increase in the degree of decision validity on the model choice for formalizing the actors' interaction in virtual communities and the corresponding model of synergistic counteraction to information security threats in the social networking services. Mamdani algorithm was chosen to reduce the degree of uncertainty in decision-making by a national information security expert on the functioning of the decision support system.

The structure of the system was developed, input and output linguistic variables were defined, to reflect the relationship between which a hierarchical tree of decisions was built, a knowledge base in the form of rules of fuzzy production rules was formed. The model of the decision support system based on the fuzzy derivation of the *MatLab Fuzzy Logic* environment was also built and an example of its application using the data on the impact of destructive information on social networking services' actors to form a negative public opinion about Ukraine's Euro-Atlantic integration was used. The advantage of the developed model of the system is the ability to scale and further supplement with new models of actors' interaction and synergetic management of interaction in virtual communities.

3.7 COUNTERACTING THE STRATEGIC MANIPULATION OF PUBLIC OPINION IN DECISION-MAKING BY ACTORS OF SOCIAL NETWORKING SERVICES

Social networking services provide many opportunities to hide the identity of users and therefore facilitate manipulation of public opinion [116–118]. Of particular importance is the impact of the social networking service on the decision-making processes of service users, for instance, during election races. For example, research by Internews-Ukraine analysts in cooperation with Singularex on the impact of social media on politics in Ukraine [119] has shown that the chance of achieving success through the use of social networking services by political forces has been given in elections is significantly increasing.

This fact was confirmed in studies [120] on information operations' impact during the presidential election in the USA in 2016. Political agitation, presented as information about the simple lifestyle and activities of candidates and political forces, has a significant impact on voters. Despite the growing number of social networking services' users, their demand to demonstrate their own political will, the existence of conflict between representatives of different political movements,

hiding their intentions from the enemy, and decision-making by actors is carried out in conditions of uncertainty. As a result, game theory models of democracy can be used to describe the influence of social networking services content on actors' decision-making processes. In decision-making processes, some conflicts may arise due to indistinct subjective choices. Research on this problem has led to the formulation of Arrow's theorem. This theorem is about the impossibility of democracy as a collective choice (the theorem of impossibility) [121–123]. Arrow's theorem proves that democratic elections cannot be called fair. However, their results adequately turn the votes of individual voters into the will of the entire nation. As a result of this approach, fair elections involve voters expressing their independent judgment about candidates. However, the independence of such actors' suggestions in the social networking services cast doubt on because of systematically disseminating targeted content to influence the public consciousness. Therefore, a promising field of research is to analyze the specifics of strategic manipulation of decision-making by actors in social networking services. The research aims to improve the security of the social networking services information space for social communications by developing effective measures to counteract strategic manipulations in decision-making by actors.

Social networking services act as a platform for actors to express their own opinions and fulfill the right to free speech. Such services provide the means to conduct user surveys. Surveys are one of the most effective types of content to establish a strong connection with the actor's audience and get their opinion on the activities of the virtual community. In the future, using the results of actor surveys on social networks will help to improve the quality of content or services provided. Furthermore, the survey provides actual data that can be applied to make optimal decisions by the actors and the administrators of social networking services' pages. Tasks for which it is expedient to use actor surveys in social networking services [124]:

– they help to get the actors' reactions to information or event. There is no need to conduct other types of surveys, and obtaining a generalized opinion of the actors on a given question does not require additional costs;

– displaying the needs of the audience of social networking services' actors. Conducting such surveys is efficient in determining audience expectations and requests. The results can be applied not only to create content but also, for example, to create an image of a new political force and its slogans and to improve business processes. In this way, knowing the actors' needs makes it possible to meet them;

– self-development of the community. Surveys increase the actors' involvement and encourage participation in discussions. At the same time, the actor feels like an essential part of the virtual community. The actor recognizes his/her ability to influence the processes that occur not only in the information space of social networking services but also in real life.

These surveys are of particular interest to citizens because they signal that there are some pressing problems in society. Therefore, social networking services serve as the leading tool for interaction between the public, the state, and public organizations. In such cases, the most trusted survey platforms are those with a broad audience. Social surveys in social networking services are indispensable for analyzing public opinion.

However, the intruder uses technologies to influence actors during the preparation, conducting, and publishing of such surveys on social networking services. In particular, among the most common ones, it is possible to highlight the following [125]:

— the use of language in questions that guides the respondent to a predetermined answer;

— covering up the inadequacy of the sample of respondents and the unreliability of the results obtained;

— covering up the specifics of the research methodology. The consequence is distorted survey results;

— manipulations when visualizing survey data to distort the actor's view of the phenomena or processes under study;

— distorted use of survey data in the headlines of social networking services publications.

These manipulations are also effectively combined with technologies for information and psychological impact on actors. For this purpose, the technologies of information and psychological influence and impact technologies are used to conduct sociological research.

In the case of strategic manipulation of actors in the social networking services, the function F does not reflect a wright ordered list of alternatives chosen by the survey participants. As a result, the final decisions on the survey data do not adequately reflect the opinion of social networking services users. In other words, the profile Ω turns into a profile $\tilde{\Omega}$, moreover $\Omega \neq \tilde{\Omega}$. Then the function F turns into $\tilde{F}$, and $F \neq \tilde{F}$ [126–128].

As a result of strategic manipulations in the social networking services, not only the genuine profile of the actors' preferences of the existing alternatives Ω becomes unknown, but also the function F that has used to make objective and unbiased decisions R. Under such conditions, conducting an actors survey in the social networking services to monitor users' opinions makes no sense.

The primary purpose of the actors' participation in the social networking services surveys is their interest in the voting procedure and their influence on the voting results — decision-making. The summary of research results by S. Vasilyev [128] allows to state that if the actor in the social networking services is considering the collective ranking of alternatives as a result of the survey, this goal includes two components:

— implementation by the actor of his/her preferences among the many alternatives given;

— one way for an actor to demonstrate his or her choice from the alternatives in an social networking services provided that he or she has no other way to show it.

The purpose of an actor's participation in the social networking services survey has defined under the following conditions [128]:

— the actor's participation in the survey using social networking services means has carried out to implement his/her preferences regarding the chosen alternative in the future, due to making appropriate decisions based on the survey results;

— as a result of social networking services actors' a_M choice alternatives α_1 and α_2, the survey results do not change — the relevant lists $\Omega'(\Omega_{a_1}, \Omega_{a_2}, ..., \Omega_{a_M})$ and $\Omega''(\Omega_{a_1}, \Omega_{a_2}, ..., \Omega_{a_{M+1}})$ are ordered and, provided that the actor a_{M+1} is indifferent to α_1 and α_2;

– as a result of the survey of actors a_M supporting alternatives α_1 and α_2 the lists $\Omega'(\Omega_{a_1}, \Omega_{a_2}, ..., \Omega_{a_M})$ and $\Omega''(\Omega_{a_1}, \Omega_{a_2}, ..., \Omega_{a_{M+1}})$ are ordered and do not change if an actor a_{M+1} did not take part in the survey.

The second and third conditions are similar and mean that actors' indifference to alternatives when conducting interviews in the social networking services is no different from ignoring them. Based on the research results [125, 128], we've formulated practical recommendations to counteract strategic manipulation in the social networking services for different types of surveys [129]. The results are presented in **Table 3.15**.

● **Table 3.15** Recommendations for conducting surveys on social networking services

Survey type	Number of survey participants	Number of alternatives	Recommendations
Choosing an alternative	$M > 2$	$N \geq 2$	ensure that no reliable information on the results of the actor' survey has been published in the social networking services; the use of precise alter native wording in the survey, which will be certainly recognizable by the participants
Rating survey on a continuous scale	$M \geq 3$	$N \geq 2$	ensure that no reliable information on the results of the actor' survey has been published in the social networking services; ensure that the social networking services do not provide any information on possible survey results

Thus, to counteract strategic manipulations in conducting interviews with actors, it is necessary to ensure that the social networking services don't contain information about the survey results. Once the results have been published, the requirement is to specify the survey methodology and sample data.

One of the most popular ways to monitor public opinion on selected essential issues is conducting social networking services surveys. The results of the surveys are used for further decision-making by actors in real life. Therefore, intruders use survey procedures and their results to manipulate public opinion. For the first time Arrow's paradox is used for formalizing the impact of strategic manipulation on the results of selecting alternatives when conducting social networking services surveys. It can counteract strategic manipulations by preventing possible poll results from being announced in advance. This approach helps to prevent the informational and psychological impact on the opinion of social networking services actors with «spiral of silence», «herd instinct», and «opinion leader» profiles.

4 INTRODUCTION PROBLEMS OF PHYSICAL ACCESS TO CRITICAL INFRASTRUCTURE AND PRE-PROCESSING OF DATA

ABSTRACT

The biometric security system that works to authenticate users based on a comparison of their fingerprints and certain templates stored in a biometric database are proposed. A method for determining the contour based on the passage of a curve and the filtering function of contour lines has been developed. The stage of skeletal identification is analyzed in detail. The Ateb-Gabor method with wave thinning has been developed. The performance of skeletal algorithms such as the Zhang-Suen thinning algorithm, the Hilditch algorithm, and the Ateb-Gabor method with wave decimation is analyzed. The presented results of experiments with biometric fingerprints based on the NIST Special Database 302 database showed the effectiveness of the proposed method. The software and firmware were developed using the Arduino Nano.

Problems of physical access to critical infrastructure for biometric information protection systems have been developed. The theory of pre-processing of data on filtering of biometric images is developed. A system of biometric protection has been built, which works on the basis of comparison of biometric prints and reveals similarities with a certain template, which is stored in a biometric database. The stage of skeletonization is developed and the wave algorithm of thinning which is realized after Ateb-filtration is offered. The propagation of the wave on the curve is considered in detail. Software for skeletonization based on Ateb-Gabor filtration has been developed. A two-dimensional Ateb-Gabor filter is used for image filtering. It is a harmonic function multiplied by the Gaussian function. The intellectual analysis of data of comparison of the scanned fingerprint with a template by the k-means method is carried out. Good puncturing characteristics are reached. Experiments of biometric prints based on NIST-14 showed the effectiveness of the proposed method.

KEYWORDS

Physical access, critical infrastructure, fingerprints, biometric protection, identification system, Ateb-Gabor algorithm.

Fingerprints are detailed, almost unique, difficult to change and stable during a person's life, which makes them suitable for the role of long-term markers of human identification.

Skeletonization algorithms for binary images are often called refinement algorithms, and discrete skeletons are also called skeletons.

The skeleton can be mathematically defined as follows. If a point PP has more than one nearest neighbor, PP is called the spanning point of the set RR [130]. The union of all spanning points is called a spanning bridge. It follows that spanning points are the centers of circles completely

covered by the set, and there are no circles with the same center and large radius covered by the set. It can be ascertained that the ostriches are extremely sensitive to noise, as any small disturbance of the boundary not only disturbs one of the ribs but also creates new ribs. If the original object is thin (narrow), the spanner contains substantial information about its shape. In the case of thick (broad) objects, this is not the case.

The transfer to the discrete plane of the notion of the middle axis is not only not obvious, but may not be possible due to complications that arise when determining the equality of distances between pixels on a discrete grid [131]. Therefore, much depends on the intuition of the algorithm's developer. One possibility is to generalize the definition into a discrete plane. It is possible to define any discrete variant of a circle and find «circles» completely covered by the set under consideration and possessing the property that there are no large «circles» with the same center, which would be covered by the given set.

4.1 GENETIC BASIS OF FINGERPRINTS

Genes control three basic schemes of human finger prints – arcs, curls and loops. Approximately 43 genetic sites are involved in the formation of a papillary pattern at the ends of our fingers. These genes are responsible not for the structure of the skin, but for the development of the limb. Therefore, the papillary pattern is closely connected with the proportions of the hand.

Finger print is unique for many reasons. After all, the West and the tracks of the epidermis at the tips of fingers occur mainly in primates and unique in each. There are basic types of patterns – arcs, curls, and loops, but in each they are shown in different ways. In particular, because of this in the criminalistics fingerprints used for identification.

But what is the reason for the uniqueness of the papillary pattern? It is known that it is formed already in the material side. About the third month of pregnancy is already clear whether the furrows on the fingers of the origin will move into arcs, curls or loops.

Looking for genes that define our finger prints, the team of scientists conducted a generic comparative study for a total of 23,000 people from different population groups. At the same time, scientists were looking for areas of the genome that can be correlated with each of the three basic patterns of papillary patterns. Results: in the Chinese genome, scientists identified a total of 43 places closely related to the papillary pattern of people of different origins. 12 of these genetic variants could be immersed in the so-called patterns – very similar usually prints of three middle fingers. Such a large number of genes involved also confirm that human finger prints are based on the complex interaction of many genetic factors. Each individual gene has a slight influence – only in combination there is an individual pattern.

Three basic schemes – curls, loops and arcs – form certain genes. For the EVI1 gene, scientists could even demonstrate this experimentally: If the mouse has changed this gene, the scheme of epidermis lifting on their skin has also changed. In humans, the EVI1 gene at early stages of

embryonic development affects the skin at the ends of the fingers and legs, as well as the cushion of the connective tissue, which marks a later form of papillary pattern.

Earlier, it was assumed that the formation of fingerprints control primarily skin genes. That is, before the formation of the skin is laid the basic scheme of our imprint on the fingers of hands and legs.

However, finger prints and growth are not only genetically related – there are also adjustments in the proportions of fingers, scientists have found out. So, people with a pattern of curl at the tips of fingers have longer ending phalanches on the average and impersonal fingers. At the sites, this correlation is even more noticeable.

Genes that control growth and proportions of hands and fingers, also determine the pattern of fingerprints. How these genes work and why at the tips of fingers form curls, loops or arcs, remains undeveloped [132].

4.2 ANALYSIS OF AUTHENTICATION SYSTEMS

Object transformations based on contour information are limited by black transformations: Zoom, move, rotate, display. However, the device of affine transformations is not always sufficient to perform complex transformations, for example, to reduce (enlarge) the individual fragments of the object [133].

Therefore, it is more appropriate to use skeletons for complex transformations, because they allow to transform individual branches of a skeleton, which are responsible for different fragments of an object, without breaking its integrity. The error of conversion is minimal. Modern biometric authentication systems with prints have one drawback – they do not see a full finger scan. They only need a small fragment, which they compare with the fragment that is in the database. Therefore, the print should match one parameter instead of ten or hundreds.

Another nuance is that some elements of the pattern are more common than others. This allows to make false prints from the most common fragments.

In the work [134] consideration is given to the removal of certain characteristics at biometric authentication and recognition. This paper presents an algorithm based on CNN for autotting fingerprints. It is used to separate fingerprints that have previously been gray and perform different patterns of removing images with noise, as well as to study the characteristics of the data to overcome background ambiguities. In the proposed method the speed of detection of fingerprints will be 0.45 s. This speed is due to the application of effective threading algorithms, saving information about the spine from hidden fingerprints. The DeepMasterprints [135] creates images that sensors see as fragments of fingerprints of real people. Working with the lowest level of protection and digital prints, the program showed results in almost 77 % of successful trials. However, as the publication notes, much more often now use the average level of protection (for example, in smartphones). There the successful result was about 23 % [136]. Such artificial prints are the most effective for the bypass of the system, in which many fingerprints are stored. The successful work of the DeepMasterprints neuronetwork is conditioned by the fact that systems of biometric

authentication only partially scan the human finger. It is enough to have only a part of the print, because everywhere there is the default repeating elements [137]. In the work [138] presented a new approach to recognition of fingerprints. Individual, special, to which the cores and deltas belong are used for the classification of fingerprints. Such an approach allows to provide the stability of recognition from singular point regions at different levels of resolution. The procedure is similar to scaling, moving, and small turns. The procedure of classification of fingerprints was built on the basis of the proposed method of detecting singular points.

Since the automatic analysis of images largely depends on the segmentation of the image, an algorithm for tracking the lines of the spine of the image of the prints is proposed. The method of frame lines of the edge, based on point categorization. The main point of the fingerprint image is detected using the adaptive method [139] proposed in this paper. The core is based on cutting the rib lines into four groups, representing four possible directions (i.e., vertical, horizontal and two diagonals).

A set of 34-dimensional features is available for fingerprint recognition and identification. The paper [140] is devoted to the issue of fingerprint segmentation. The paper proposes an online method of fingerprint segmentation based on frame difference. Segmentation is performed in the online image capture process, without using orientation information or grayscale. The background is extracted from consecutive images taken by the fingerprint sensor, and the background is removed using the frame difference. Background with fingerprints and stains can be effectively removed by the developed method.

Fingerprint image segmentation is one of the key steps in the Automatic Fingerprint Identification (AFIS) system, and how to do it faster, more accurately and more efficiently is important for AFIS. In [141] the method of Markov chain Monte Carlo (MCMC) and genetic algorithm (GA) in the segmentation of fingerprint images and proposed the method of segmentation of fingerprint images based on the Markov chain Monte Carlo and genetic algorithm (MCMC & GA). This approach has generated a random sequence of closed curves, which is considered as the boundary between the fingerprint image area and the background image area, such as the Markov chain, which uses the probability curve density (BCPDF) function as an indicator of convergence. It is then modeled by the Monte Carlo method with BCPDF as the most convergent parameter. Finally, a genetic algorithm is introduced to accelerate the convergence rate. Finally, the closed curve with the maximum BCPDF value is the ideal boundary curve. The results of experiments show that the method is reliable for poor quality images of the fingers.

The approach to the organization of control systems is described in [142, 143]. From these studies were taken data on the construction of systems, parallelization of processes in the biometric fingerprint identification system.

4.3 REVIEW AND ANALYSIS OF BIOMETRIC PROTECTION SYSTEMS

The digital form of the image is obtained by scanning with a finger sensor. Next is the preprocessing stage, which reduces the effect of noise. To determine if the correct information was

stored, a new fresh sample from the user is used to compare the saved sample for each match. Human fingerprint samples at different times are never completely similar because the user interacts with the biometric system under different circumstances, has different humidity, grease, dust, varying degrees of finger pressure, and changes in fingerprints due to injuries and age. The threshold determines whether the two patterns match. If the data obtained by comparing the digital image and the image from the template is higher than the threshold, the threshold is called a match. Take the threshold of 0.40 [144], which is the standard for the recognition system. A detailed study of the correspondence between the class and between the class helps to determine the frequency of erroneous deviation and the rate of erroneous acceptance.

The block diagram (**Fig. 4.1**) illustrates two main modes of critical infrastructure for preprocessing biometric protection data [145]. First, in authentication mode, the system compares with each other and identifies similarities with a specific template stored in the biometric database to verify that the person is the one who is eligible to log in.
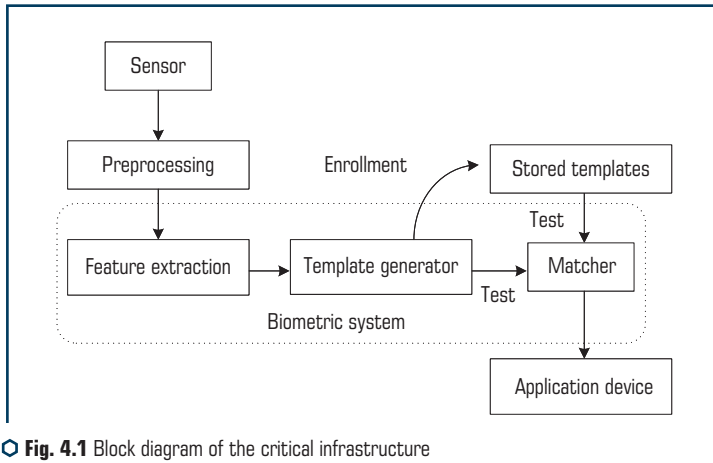
○ **Fig. 4.1** Block diagram of the critical infrastructure for pre-processing biometric protection data

The identity check takes place in three stages. At the first stage, reference models for all users are formed and stored in the database of models. In the second stage, some samples are agreed with the reference models to generate a real security assessment and calculate the entry threshold. The third stage is testing. This process can use a smart card, username, or ID, such as a PIN, to specify which template to use for comparison. Let's introduce the so-called «positive recognition» and «negative recognition». «Positive recognition» is the usual use of the test mode, when it is necessary to prevent the use of multiple people as one template.

Next, in the identification mode, the system compares «one to many» [146] with a biometric database, trying to establish the identity of an unknown person. The system will be able to

identify a person if the comparison of the biometric sample with the template in the database is within the previously set threshold. The identification mode can be used either for «positive recognition». The user does not need to provide any information about the template to be used or for «negative recognition» of the person when the system determines whether the person is who he/she claims to be.

The first time a person uses a biometric system, it is called enrollment or recording. During enrollment, biometric information from an individual is recorded and stored. With further use, biometric information is detected and compared with the information stored at the time of enrollment. To preserve a biometric system, it is important that the storage and retrieval of such systems be safe. The first unit, the sensor, is the interface between the real world and the system; it must accept all the necessary data. In most cases, this is an image acquisition system, but it can vary according to the desired characteristics. The second unit performs all the necessary pre-treatment: it must remove noise from the sensor. In the third block the necessary functions are extracted. This step is an important step, because the right functions need to be extracted optimally. A vector of numbers or images with certain properties is used to create a template. Elements of biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce file size and protect the identity of the participant [147].

The template is saved during recording. During the comparison phase, the template is passed to a comparison function, which compares it with other existing templates, estimating the distance between the ridges using the PSNR algorithm [148]. The comparison program analyzes the template with the input image. The choice of biometric data depends on the specific measurements and user requirements.

One of the stages of fingerprint authentication is the thinning stage, and then, based on thinning, skeletonization. Let's describe three methods of thinning: Zhang-Suen Algorithm, Hildich Algorithm and our proposed Ateb-Gabor algorithm, which is performed together with the wave algorithm.

4.4 PRE-PROCESSING OF DATA IN CRITICAL INFRASTRUCTURE SYSTEMS

The functional diagram of the critical infrastructure identification system is shown in **Fig. 4.2**.

The image of an object through a scanner or camera is transmitted to a light-signal converter, and then to the information system to the original image processing unit. The Image Analysis Unit is used to identify and recognize the object, determine its coordinates and position.

This unit implements contour and skeletal tracking, affine transformations, and normalization. On the basis of the information received, the comparison is carried out by the means of similarity or the identification is carried out by the correlation methods on the basis of the established bank of standards. The result of the identification is to define the parameters of the Ateb-functions, assess the document authenticity and save the processed data.
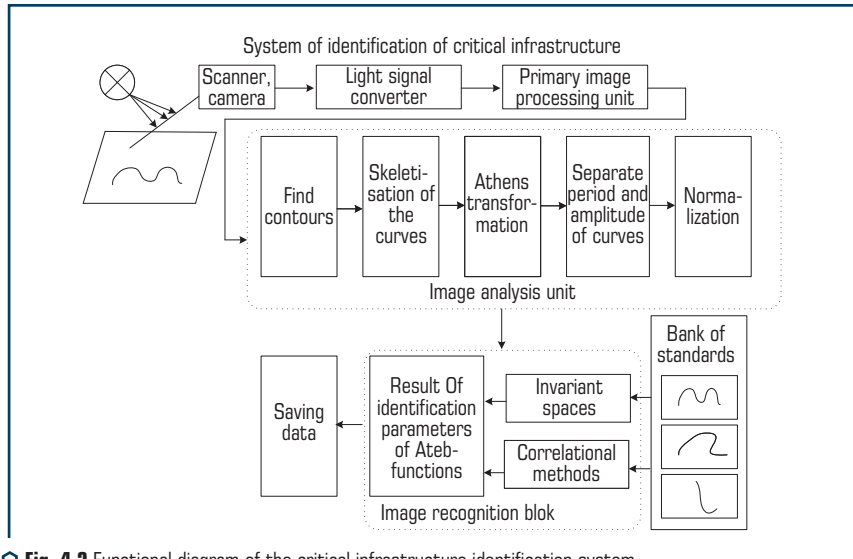
Fig. 4.2 Functional diagram of the critical infrastructure identification system

Today there are widespread systems of automated information input through different types of scanners, as well as digital cameras. The digital camera matrix provides a resolution of up to 3 megapixels per frame, and today's PCs are available in real-time mode, such as spatial flat-parallel correlation [149]. However, the ability to intelligently analyze images with computers should be much better [150]. Expert systems based on image-enabled databases require fast and reliable analysis of digitized video information in specialized image archives or in Internet databases [151]. Image processing in order to recognize them is one of the central and practically important tasks. The problem includes a number of main stages: perception of the field of view, segmentation, normalization of selected objects, recognition [152]. The main element of any image recognition problem is the answer to the question: whether these input images belong to the image class that represents this standard [153]. The answer can be obtained by directly comparing the image with the standards (or their features). However, there are a number of difficulties and specific problems [154]:

1. Images are placed on a complex background.

2. Reference images and input images differ in location in the field of view.

3. Input images do not match the standards due to random interference.

4. Differences between input and reference images arise due to changes in illumination, illumination, local interference.

5. Standards and images can distinguish geometric transformations, including affine and projective.

Different methods of segmentation, normalization and recognition are used to solve the problem as a whole and at its individual stages. The development of the identification method [155] is to

separate a single graphic element from the scanned image, normalize it and compare it with a specific reference image. Let's build reference images. In addition, the scanned image must be specially processed to select the image for comparison with the reference. This requires the use of special algorithms in the theory of image recognition, namely segmentation, skeletonization and normalization.

To identify the printed print [156] requires:

1. Each form must be presented in the format of an uncompressed tif file.

2. Documents with a resolution of about 300 dpi must be scanned for identification.

3. The document should be scanned with 256 gradations of brightness.

In the database let's store graphic primitives in the form of two graphs, which improves the quality of recognition. Graphs differ by a shift of several pixels. We do not change the scale, because the recognition is carried out with the operation of normalization, i.e., reduction to one scale.

The technology of comparing two prints consists of six stages. The first step is to improve the quality of the input scanned image. At this stage, the sharpness of the borders for background grids increases. In the second stage, the choice of orientation of the background grid, bringing to a single scale, rotation. The image is divided into square blocks. The third stage is the binarization of the print and its conversion into a black and white image (1-bit).

During binarization, the image is converted to monochrome, often to black and white. This process is called 50 % conversion. Transformation can be done by means of color separation, but in this case the final image will not be binary (black and white), but will contain 8 pure colors, representing a combination of red, green and blue, i.e. will be binary in color. If the image is in color, it may be in an RGB color separation system. It is possible to perform grayscale transformation, which consists in obtaining the brightness of each point according to the formula [147]:

$$Y = 0.3R + 0.59G + 0.11B.$$

The next step is to bring the background grid lines to a thinner look and to a thickness of one pixel of the curves. This is the selection of the contour, which is highlighted in **Fig. 4.3** darker color and plotting curves. Let's call the contour of the image a set of its pixels, around which there is an abrupt change in the brightness function. The contours of the image will be represented by lines one pixel wide.

If the original image, in addition to areas with constant brightness, contains areas with brightness that changes smoothly, then setting the contour boundary does not guarantee the continuity of contour lines: there will be gaps where the change in brightness is not sharp enough. On the other hand, there is noise in the piecewise constant image, and extra contours may be recognized, which are not desirable when creating area boundaries. Contour selection algorithms are developed and the behavior of contour lines is taken into account. Special additional algorithms can eliminate gaps and eliminate unnecessary contour lines. To highlight the boundaries, i.e., brightness differences, there are known methods: gradient method, which consists in differentiating the brightness function; wave method. Consider a fragment of an image that is scanned by the wave

method and covers several pixels at once. The window contains a small fragment. When to move the window, the fragment changes. Image processing by the wave method is shown in **Fig. 4.3**.

In the fifth stage, the image is divided into certain fixed blocks. On the curve let's find the points of maximum or minimum. Based on this, a coordinate system is built, as shown in **Fig. 4.4**. And the last stage of identification is a comparison with the reference model. The result of the identification is the establishment of the type of Ateb function and its parameters m, n [148].
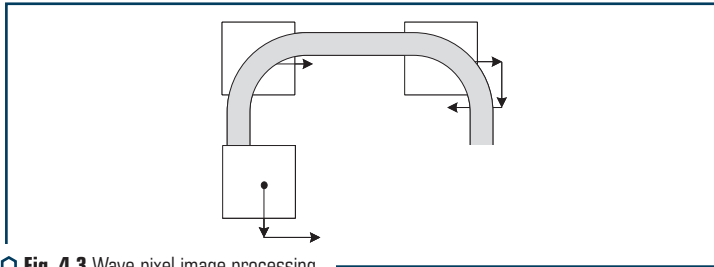
○ **Fig. 4.3** Wave pixel image processing
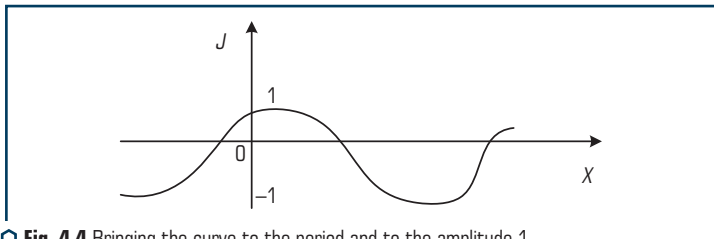
○ **Fig. 4.4** Bringing the curve to the period and to the amplitude 1

At the final stage, it is necessary to assess the reliability of the input image by comparison with the standard. For comparison with the standard, factor spaces built on the basis of different equivalence relations are considered. The equivalence relation is determined by the choice of metric in a given metric space. The result of the classification of recognized objects is significantly influenced by the types of classes. The core class or condensation class is most often distinguished in our case. In this case, all distances between objects within a factor class are less than their distances to any object that is not in that class. There are also classes such as clusters, or thickening on average. In this case, the average distance between objects within the class is less than the average distance to all other objects.

Depending on the purpose of the study, the task of classifying recognized objects can be formulated as dividing the analyzed objects into a number of groups within which they are located at a relatively short distance from each other, or as identifying the natural stratification of the population under study into separate clusters.

Distance similarity measures are used to form clusters. When used, objects are considered to be more similar to each other, the smaller the distance between them. The results of classification by different methods, as a rule, do not differ fundamentally. The choice of metrics, on the contrary, can significantly affect the results of the analysis. Therefore, for each identification let's consider different types of distances, and implement a comparison of the results. Let's consider Euclidean distances, Manhattan distances, supreme norm.

Image optimization for implementation of vector representation of information in the system of identification of critical infrastructure

To solve the problem of identifying documents protected by function-based grids, it is necessary to perform image recognition and highlight security features in the recognized image. It is known that the theory of image recognition is based on the methods of graph theory, the theory of algorithms. To solve this problem, consider the necessary mathematical apparatus. Let's consider some definitions. Consider a raster black and white image of size $p \times q$ pixels (dots). For certainty, without reducing the generality of reasoning, let's assume $p < q$. Let's match it to the matrix.

Definition 4.1. A raster black-and-white image R is a matrix of size $p \times q$, the elements of which can be zeros and ones. Let's assume that the zeros correspond to the white dots of the background, and the ones to the black dots of the raster image:

$$R = r_{ij} \left| r_{ij} = \{0,1\}, i = 1,\ldots,p; j = 1,q. \right.$$

Definition 4.2. The object in the image is the set RO of those elements R, corresponding to the black dots of the raster:

$$RO = r_{ij} = 1 \left| i = 1,\ldots,p; j = 1,\ldots,q. \right.$$

Definitions 4.3. The background in the image is considered to be the set of RF elements R, corresponding to the white dots of the raster:

$$RF = \left\{ r_{ij} = 1 \left| i = 1,\ldots,p; j = 1,\ldots,q. \right. \right.$$

The following properties of the entered sets for black-and-white images are obvious:
Property 4.1. The sets of the object and the background do not intersect:

$$RO \cup RF = \varnothing. \tag{4.1}$$

Property 4.2. Combining an object and a background creates an image:

$$RO \cup RF = R. \tag{4.2}$$

Let's introduce the *XOY* coordinate system, which corresponds to the numbering of matrix elements. Let's consider the upper left point O(0,0) of the raster image plane to be the starting point of the coordinate system. Let's consider the horizontal column number of the matrix, and the vertical row number of the matrix.

For example, the coordinate (3, 5) corresponds to the matrix element at the intersection of the third row and the fifth column and is at the same time the image pixel image.

Definition 4.4. The distance between the points of the image will be calculated by the formula:

$$p\left(x_{ij} - x_{kl}\right) = \sqrt{\left(k - i\right)^2 + \left(l - j\right)^2}. \tag{4.3}$$

Theorem 4.1. The distance $p\left(x_{ij} - x_{kl}\right)$ given by formula (4.3) satisfies the axioms of distance.

Definitions 4.5. Around a certain point of the image let's consider the set of those elements of the image that satisfy the following condition:

$$R_\varepsilon\left(x_{ij}\right) = \left\{x_{kl} \middle| p\left(x_{ij}, x_{kl}\right) < \varepsilon, \ \varepsilon = 0,1,\ldots,p. \right. \tag{4.4}$$

An example of the circumference is shown in **Fig. 4.5**.
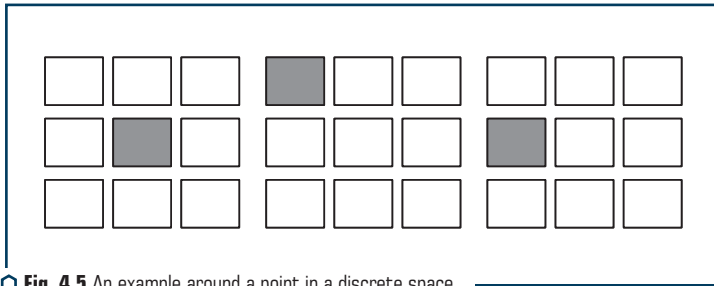
○ **Fig. 4.5** An example around a point in a discrete space

Definition 4.6. The end point x_{ij} of an object will be considered to be its end point in any neighborhood which contains points from the object and the background. Points $x_{ij} = 1$ at which by definition let's consider extreme:

$$x_{ij} = \left\{\forall \varepsilon, \exists R_\varepsilon \middle| x_{kl} \in RF \cap R_\varepsilon \wedge x_{\alpha\beta} \in RO \cap R_\varepsilon\right\}. \tag{4.5}$$

Definition 4.7. The set of all extreme points of the object is denoted by *K* (**Fig. 4.6**). The set of points of an object without extreme points will be called internal points and denote *RV*:

$$RV = \left\{x_{ij} \middle| y_{ij} \in RO / K\right\}.$$
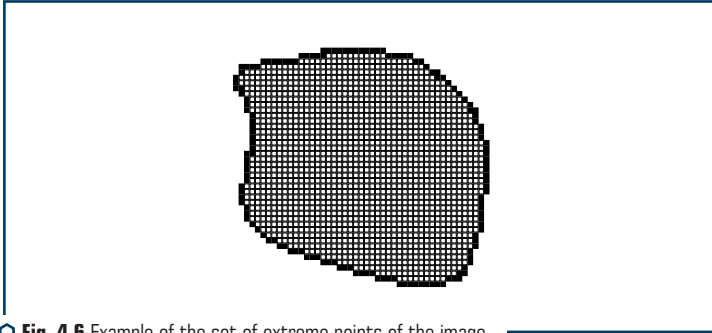
○ **Fig. 4.6** Example of the set of extreme points of the image

Definition 4.8. A segment on an object is a subset of points *RV* which distance from the extreme points of the object is not greater than a predetermined value of *d*:

$$V = \left\{ x_{ij} \middle| p\left(x_{ij} - x_{kl}\right) < d, \ x_{pq} \in K \right\}.$$

As can be seen in **Fig. 4.7** segment has two ends A, B, which belong to the inner points. Let's mark a segment with its ends. The length of the segment will be considered the distance between its ends.
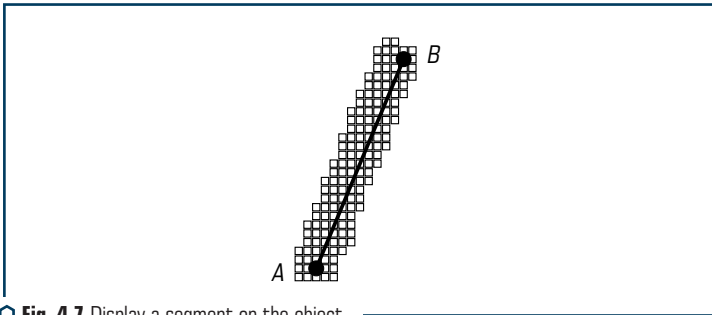
○ **Fig. 4.7** Display a segment on the object

Definition 4.9. The intersection of segments will be considered to be the representation of segments in the form of segments of shorter length that have a common end (**Fig. 4.8**):

$$AB = AO \cup OB, CD = CO \cup OD, O \in \left(AB \cap RV\right), O \in \left(CD \cap RV\right).$$

Consider a set of connected segments $V = V_1 \cup V_2 \cup \ldots \cup V_N$. Denote the set of ends of these segments *E*. Let's consider a couple $G = \left\{V, E\right\}$.
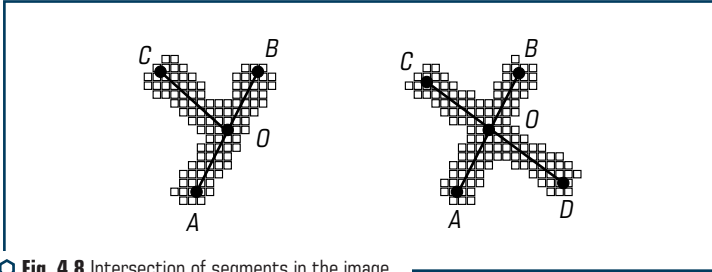
○ **Fig. 4.8** Intersection of segments in the image

Definition 4.10. The set will be called a graph. In this case, let's call the set of edges of the graph — the set of vertices of the graph.

Consider the edge of two vertices S and a vertex T. In the general case, $\{S,T\} \neq \{T,S\}$, where $\{S,T\}, \{T,S\} \in V$. In this case, the graph G is called an oriented graph. To solve the problem of image recognition, which can be attributed to the class of geometric problems, it is sufficient to consider undirected graphs. In the future let's believe that $\{S,T\} = \{T,S\}$. An undirected graph is said to be finite if the set of its vertices is finite. Since the image recognition problem is contained in the exchange area, the constructed graphs will have a finite number of nodes. A graph G is called flat if it can be represented on a plane so that the edges have no points of intersection other than the vertices. Graphs that meet image recognition problems are always placed in a two-dimensional plane and are so-called planar or flat graphs. Therefore, in the future let's consider only undirected finite flat graphs and will omit the adjectives «undirected» «finite» «flat». In [29] it was noted that image recognition problems are naturally described by undirected finite flat graphs.

Definition 4.11. The route of a graph is a sequence of edges $V_1, V_2, \ldots, V_N$ in which every two consecutive edges V_i, V_{i+1} are different and have a single common vertex. The same edge can occur in the route several times. The vertex V_1 of the edge that does not belong to V_2 is called the beginning of the route. The top of the edge V_N that does not belong to V_{N-1} is called the end of the route. Two vertices S, T are said to be connected if there is a route beginning with S and ending with T. If the vertices S and T are connected and $S=T$, then the route is called cyclic.

Definition 4.12. A graph G is said to be connected if all its vertices are connected.

The problem of establishing the connectivity of a graph [157] is extremely important for image recognition tasks.

The main characteristics of each graph are the number of its vertices N and the number of its edges K. If $V_1 \in V$ it looks like $V_1 = \{S,T\}$ an edge is called incident to the vertex S, and each of the vertices S, T is called incident to the edge V_1. Vertices S, T that belong to some edge are called adjacent. The degree of the vertex S of a graph is called the number of edges incident to it, and this value is denoted by degree (S). The degree of the vertex determines the importance of the corresponding node in recognition problems. A vertex S is called finite if its degree is 1, i.e., degree $(S)=1$.

Let's denote the sum of the powers of the vertices of the graph by r. The following statements are made.

Property 4.3. The sum of the powers of the vertices of a finite graph is twice the number of edges $r = 2 \times K$.

Each edge connects two vertices and is therefore counted in the sum of the powers of the vertices twice. So, the sum of the powers of the vertices is twice the number of edges. Property 4.3 is proven.

Property 4.4. The number of vertices of an odd degree of an arbitrary graph is an even number. Divide the sum of the powers of the vertices of the graph into two terms $r = r_1 + r_2$, where r_2 is the sum of the powers of the even power, and r_1 is the sum of the powers of the odd power. Even number. If the number of vertices r_1 of odd degree would be odd, then the sum r would be odd. This contradicts property 4.3. Property 4.4 brought.

Denote the maximum number of edges in the graph by Z_{max}. Then the following statement is true.

Property 4.5. A graph G with N nodes contains no more $N(N-1)/2$ edges, or a fair inequality $Z_{max} \leq N(N-1)/2$.

The total number of possible pairs of vertices is N_2. This takes into account the N connections with oneself and all pairs of connections are taken into account twice. Therefore, the maximum possible number of connections is equal $(N^2 - N)/2 = N(N-1)/2$, which proves the validity of property 4.5.

The concept of graph saturation is important for image recognition problems.

Definition 4.13. Let's consider the value η – the saturation of the graph by the formula:

$$\eta = \frac{r}{N}.$$

Let's assume that the graph is saturated if the inequality $\eta \geq N$ holds and sparse, or unsaturated if $\eta < N$. In image recognition problems, graphs are usually sparse [161]. This feature of graphs c is extremely important when choosing algorithms for solving image recognition problems, because it is known that some algorithms coincide much faster on sparse graphs [162].

Definitions 4.14. The thickness of the rib will be considered the distance between the nearest extreme points of the rib.

A graph G will be called edge-weighted if each of its edges V corresponds to a positive real number $w(V)$, or in other words a mapping from a set w of edges to a set of real numbers is given w: $V \rightarrow R$. The number is called the weight of the rib. The sum of the weights of all edges will be called the weight of the edges of the graph and denote $w(G)$.

When considering a graph of image recognition problems, it is advisable to enter into consideration the weights that correspond to each vertex of the graph. A graph G will be called vertex-weighted if each of its vertices corresponds to a real number, or in other words a mapping w from a set of vertices to a set E of real numbers is given w: $E \rightarrow R$. The number $w(S)$ is called the weight of the vertex S. The sum of the weights of all vertices will be called the weight of the vertices of the graph and denote $w(G)$.

In image recognition problems, let's usually use weighted graphs.

Let's consider the following mappings.

Display that takes into account the length of the rib $V=S\times T$:

$$w(V)=\rho(S,T).$$ (4.6)

Mapping that takes into account the thickness of the edge $V=ST$ of the distance between the nearest extreme points of the edge (**Fig. 4.9**).
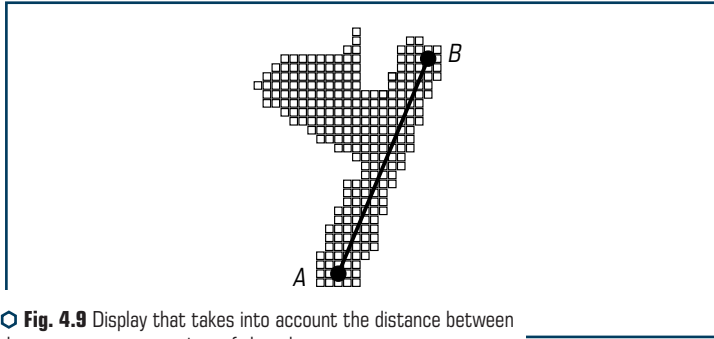
$$w(V)=s(V).$$ (4.7)

○ **Fig. 4.9** Display that takes into account the distance between the nearest extreme points of the edge

Let's consider the mappings of the weights corresponding to each vertex of the graph. Display that takes into account the coordinates of the vertex S:

$$w(S)=\Theta(S)=(x,y).$$ (4.8)

Representation of the graph in the form of an incidence matrix.

For the computer representation of graphs and the implementation of calculations on graphs, let's use the representation of the graph in the form of an incidence matrix. Let's suppose a graph G with vertices N. Let's renumber the set of vertices $E=\{S_1,...,S_N\}$. Incidence matrix. graph will be called a square matrix $A=[a_{ij}]$, N-th order.

Vertices S_iS_j are called adjacent if there is an edge $S_iS_j\in V\subset E\times E$. For oriented graphs, the adjacency relation on the set of its vertices is symmetric. Therefore, the incidence matrix of the oriented graph is symmetric.

In the case of an edge-weighted graph with a given reflection by formulas (4.8)–(4.10) the incidence matrix $A=[a_{ij}]$.

Let's use the introduced tools to solve identification problems.

4.5 ALGORITHMS FOR THINNING THE CRITICAL INFRASTRUCTURE IDENTIFICATION SYSTEM

Thinning algorithms implement a bit image with maximum shape adherence and image conversion to the skeleton relative to the structure of the full image [163].

The stage of construction of the skeleton of the figure is usually preceded by several auxiliary stages. This is a pre-treatment – removal of fine noise and binarization of the image. Binarization is the process of converting color and halftone images into two colors. For binarization threshold processing, methods of point transformations, convolutions, strengthening of edges, allocation of low-frequency and high-frequency components of the image are used.

Zhang-Suen algorithm

One of the best known is the Zhang-Suen thinning algorithm [164]. It is one of the most widely used thinning algorithms.

The algorithm is a 2-pass algorithm, so it performs two sets of checks for each iteration. These checks remove pixels from the image. The essence of the method is as follows: The checks are designed so that the first check starts from the lower right corner of the image, and the second check starts from the upper left corner. Zhang-suen's algorithm works in the area of black pixels with eight neighbors. This means that pixels found at the edges of the image are not analyzed. For those pixels that are analyzed, the order is shown below (**Fig. 4.10**). P_1 is the black pixel being analyzed.

P_9	P_2	P_3
P_8	P_1	P_4
P_7	P_6	P_5
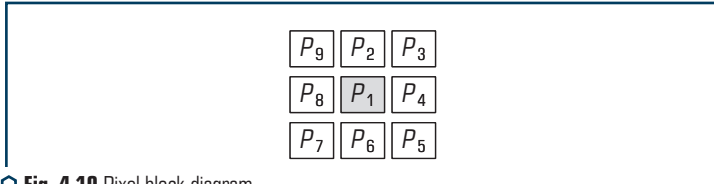
○ **Fig. 4.10** Pixel block diagram

$A(i, j)$ is the number of transitions from white to black in a sequence of eight neighbors around the central pixel, where the sequence begins and ends on the same neighbor (forming a complete circle $P_2 \geq P_3 \geq P_4 \geq P_5 \geq P_6 \geq P_7 \geq P_8 \geq P_9 \geq P_2$). From **Fig. 4.10** it can be seen that moving clockwise around P_1, and as a result P_2 should appear twice ($P_2 \geq P_3$ and $P_9 \geq P_2$ transitions).

$B(i, j)$ = number of black pixels among the eight neighbors around the central pixel.

Select a pixel to delete if it meets all of the following conditions:

Passage 1:

1) the pixel is black and has eight neighbors;

2) $2 \leq B(i, j) \leq 6$;

3) $A(i, j) = 1$;

4) at least one of the northern, eastern and southern neighbors is white;

5) at least one of the eastern, southern and western neighbors is white.

Passage 2:

1) the pixel is black and has eight neighbors;

2) $2 \leq B(i, j) \leq 6$;

3) $A(i, j) = 1$;

4) at least one of the northern, eastern and western neighbors is white;

5) at least one of the northern, southern and western neighbors is white.

Only steps 4 and 5 change between passes. If a pixel is selected for deletion via Pass 1 or Pass 2, it is deleted. These passes are both repeated until a pixel to delete is selected.

Hilditch skeleton

Consider a group of 3×3 pixels (**Fig. 4.11**). Denote the central pixel by p_1, and all its neighbors by $p_2 - p_9$, respectively.
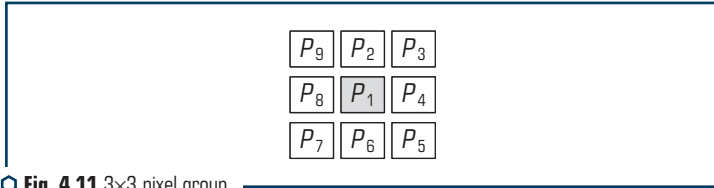
○ **Fig. 4.11** 3×3 pixel group

During scanning, the decision to change the color is made relative to the pixel p_1 [150]. To answer the question of whether to leave the dark color pixel p_1 in the skeleton, or change its color to white, it is necessary to calculate two functions:

$B(p_1) =$ number of non-zero neighbors for p_1.

$A(p_1) =$ number of pairs $\{0, 1\}$ in the sequence $p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_2$.

Examples of different configurations of pixel p_1 neighbors and functions for it are shown in **Fig. 4.12**.
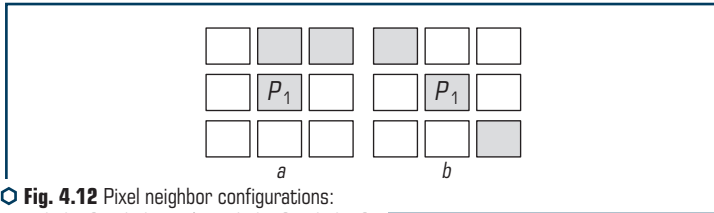
○ **Fig. 4.12** Pixel neighbor configurations:
$a - B(p_1) = 2, A(p_1) = 1$; $b - B(p_1) = 2, A(p_1) = 2$

Hildich's algorithm uses a 3×3 pixel block.

Hildich's algorithm consists of performing several passes on a template and on each pass, the algorithm checks all pixels and decides whether to change the pixel from black to white, if it satisfies the following four conditions:

$2 \leq B(p_1) \leq 6$;

$A(p_1)=1$;

$p_2 \times p_4 \times p_8 = 0$ or $A(p_2)! = 1$;

$p_2 \times p_4 \times p_6 = 0$ or $A(p_4)! = 1$.

Stop when nothing changes (more pixels cannot be deleted).

Consider each of the above conditions separately.

Condition 1: $2 \leq B(p_1) \leq 6$.

This condition combines two subconditions, first, that the number of nonzero neighbors p_1 is greater than or equal to 2, and second, that it is less than or equal to 6. The first condition ensures that no pixel endpoint and isolated point will be deleted, i.e., any a pixel with 1 black neighbor is an endpoint pixel. The second condition ensures that the pixel is a limit pixel (**Fig. 4.13**).
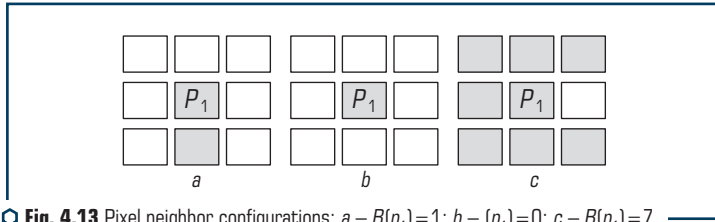
○ **Fig. 4.13** Pixel neighbor configurations: $a - B(p_1)=1$; $b - (p_1)=0$; $c - B(p_1)=7$

In **Fig. 4.13** shows that if $B(p_1)=1$, then p_1 is the endpoint of the skeleton and should not be removed. If $B(p_1)=0$, then p_1 is an isolated point, and it should also be stored, if it is noise, removing the pixel is not a task of skeletonization. If $B(p_1)=7$, p_1 is no longer on the edge of the figure, and therefore it should not be a candidate for removal.

This is a connectivity test. In fact, if to consider the following images, where $A(p_1)>1$, it is possible to see that changing p_1 to 0, the pattern will be separated (**Fig. 4.14**).

Condition 2: $A(p_1)=1$ (**Fig. 4.14**).
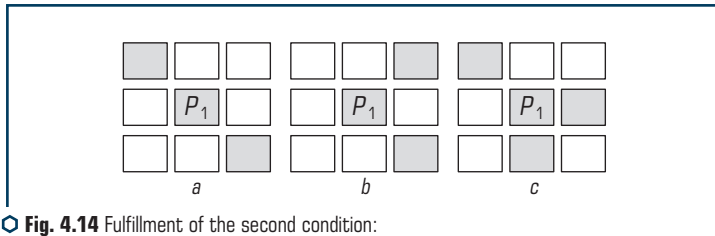
○ **Fig. 4.14** Fulfillment of the second condition:
$a - A(p_1)=2$; $b - A(p_1)=2$; $c - A(p_1)=3$

Condition 3: $p_2.p_4.p_8 = 0$ or $A(p_2)! = 1$ (**Fig. 4.15**).

This condition ensures that 2-pixel wide vertical lines will not be completely blurred by the algorithm (**Fig. 4.16**).
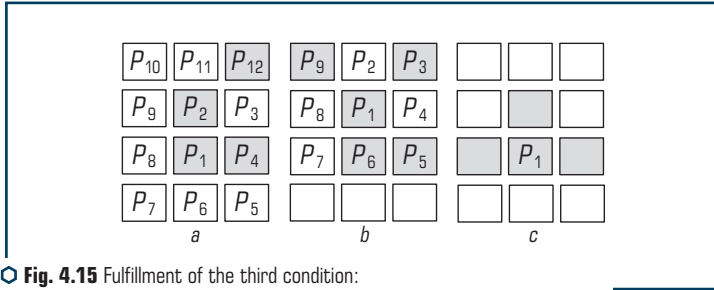
○ **Fig. 4.15** Fulfillment of the third condition:
$a - A(p_2)$ is not equal to 1; $b - p_2 \times p_4 \times p_8 = 0$; $c - p_2 \times p_4 \times p_8 \neq 0$ and $A(p_2) = 1$
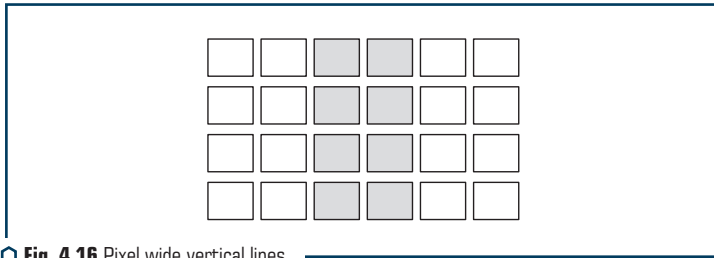

○ **Fig. 4.16** Pixel wide vertical lines

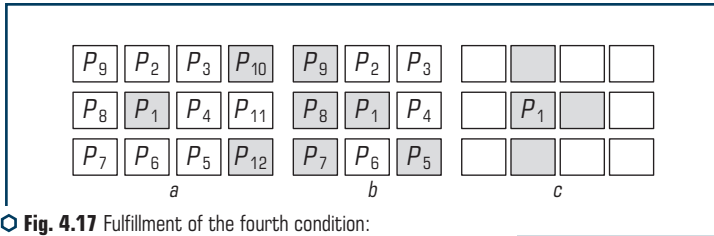Condition 4: $p_2 \times p_4 \times p_6 = 0$ or $A(p_4)! = 1$ (**Fig. 4.17**).

○ **Fig. 4.17** Fulfillment of the fourth condition:
$a - A(p_4)! = 1$; $b - p_2 \times p_4 \times p_6 = 0$; $c - p_2 \times p_4 \times p_6! = 0$ and $A(p_4) = 1$

This condition ensures that 2-pixel horizontal lines are not completely blurred by the algorithm (**Fig. 4.18**).

This is a parallel-serial algorithm. This is in parallel, because in one pass all pixels are checked at the same time and a decision is made whether to delete each of the checked pixels. It is consistent because the step just mentioned is repeated several times until there are no more pixels to replace.

However, Hildich's algorithm was not an ideal skeletonization algorithm, as it does not work on all templates. In fact, there are patterns that are completely erased by the algorithm (**Fig. 4.19**).
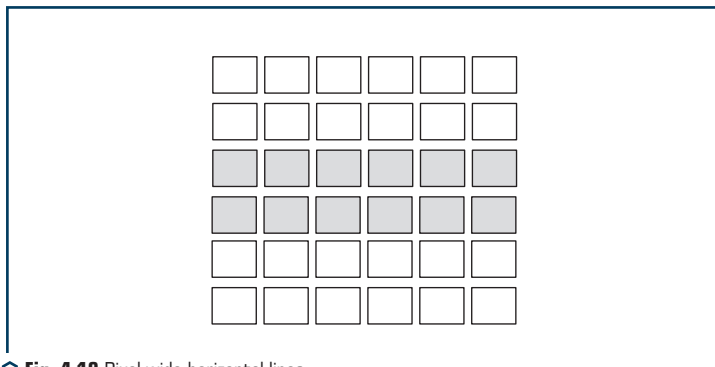
○ **Fig. 4.18** Pixel wide horizontal lines
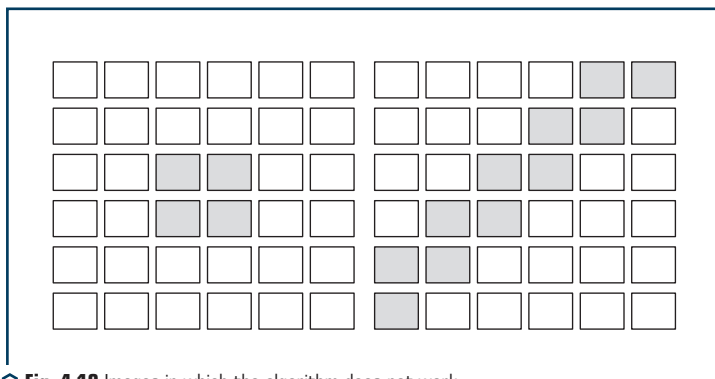
○ **Fig. 4.19** Images in which the algorithm does not work

Implementation of the algorithm of Zhang-Sun and Hildich

The block diagram of the Zhang-Sun algorithm is shown in **Fig. 4.20**.

It is necessary to first import the scanned image and convert it to a two-dimensional binary array. The software is implemented in Python, so let's use OpenCV and NumPy libraries [162].

Let's first import images in grayscale. After that, binarize the threshold value to convert the image to bitmap mode; any pixel with a value greater than 0 will be changed to 255.

Currently, the image can be represented as a two-dimensional array containing 0 for black pixels and 255 for white pixels. To build a program to thin this array, convert the array to black=0 and white=255. Any 0 in the original threshold array will be converted to 1 (True), and non-zero values – 0 (False).

After creating the conditions of the algorithm, it is already possible to sort the pixels of the image, checking each pixel for conditions and sorting it until convergence is achieved.
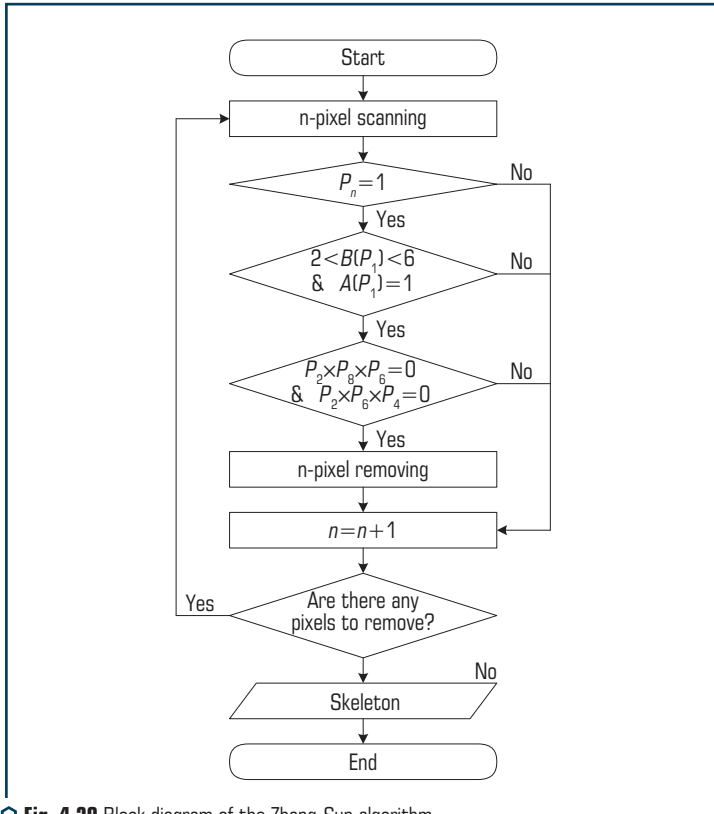
The scheme of the algorithm is shown in **Fig. 4.21**.

○ **Fig. 4.20** Block diagram of the Zhang-Sun algorithm
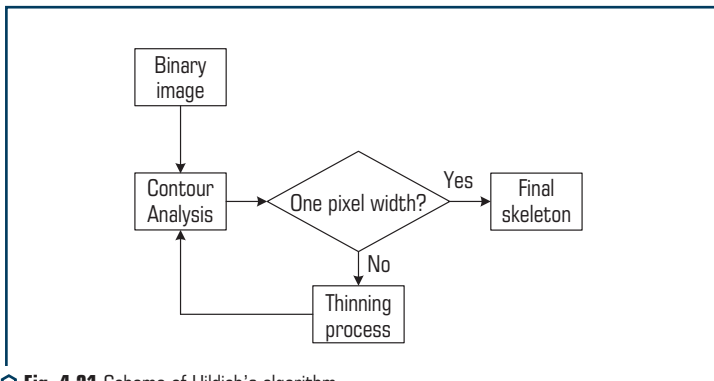

○ **Fig. 4.21** Scheme of Hildich's algorithm

### Implementation of the Ateb-Gabor algorithm

In this study, skeletonization based on Ateb-Gabor filtration [165] and thinning by the wave algorithm were implemented. The most common means of assessing image quality is the ratio of peak signal to noise (PSNR). A distinctive feature of this method, from PSNR, is that it takes into account the «perception of error» by taking into account the structural changes in information. The idea is that pixels have a strong relationship, especially when they are close in space. These dependencies carry important information about the structure of objects and the scene as a whole [148, 166].

Analysis of binary fingerprints that are omitted in the biometric identification system and recognized by it are shown in **Fig. 4.22** without filtering and with tracing developed by the method of Ateb-Gabor. As it is possible to see from **Fig. 4.23** show skeletonized images from the NIST 24 database by Zhang-sung algorithm [167]. This way the images are more noise free. **Fig. 4.24** show skeletonized images from the NIST 24 database by Hildich's algorithm.
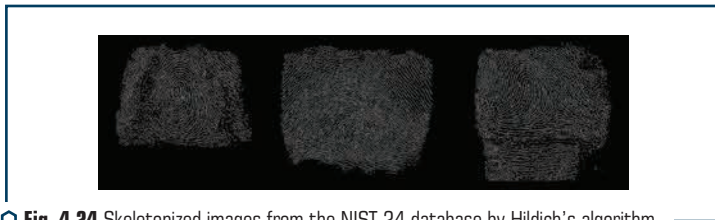
The result of the considered algorithms is the skeletons of fingerprint images. Their comparisons are presented in **Fig. 4.25**.
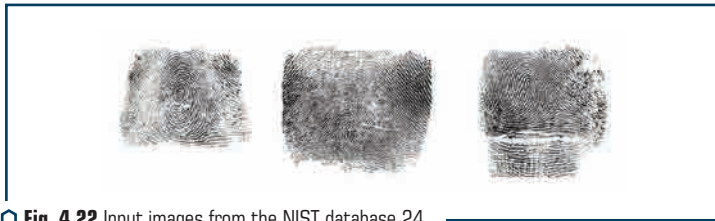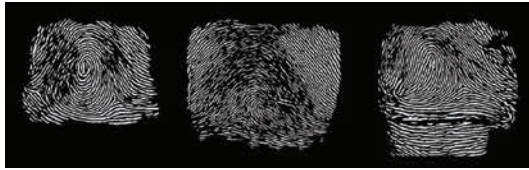

○ **Fig. 4.22** Input images from the NIST database 24
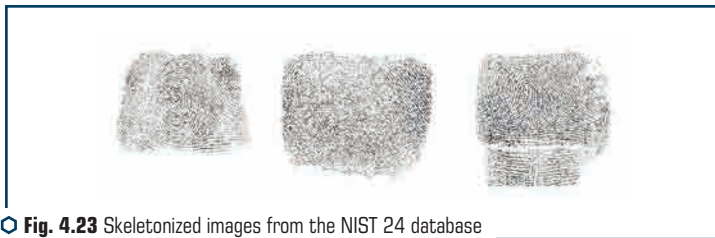
○ **Fig. 4.23** Skeletonized images from the NIST 24 database by Zhang-sung algorithm

○ **Fig. 4.24** Skeletonized images from the NIST 24 database by Hildich's algorithm

○ **Fig. 4.25** Skeletalized images from the NIST 24 database
by the Ateb-Gabor filter and the wave thinning method

The schedule of Ateb-Gabor functions is a schedule of modulated sine wave fragments. The length of the fragments for all frequencies is constant, which gives a different number of oscillations for different harmonics. It follows that the Gabor function, which is well localized in t and k space, cannot be the basis of the wavelet transform, since the basis constructed on its basis does not have the property of self-similarity [162].

The execution time of Hilditch's algorithm, Zhang-Sun Algorithm, Ateb-Gabor with wave algorithm is calculated. It is shown that the execution time of Ateb-Gabor with the wave algorithm, although longer (**Table 4.1**), but the quality is much better (**Fig. 4.25**).

● **Table 4.1** The succession algorithm execution

The name of the algorithm	Time of operation when implemented once	Time of operation when implemented twice	Time of operation when implemented three times
Hilditch algorithm	2.03 ms	1.76 ms	1.74 ms
Zhang-Sun Algorithm	3.42 ms	2.56 ms	2.95 ms
Ateb-Gabor with wave algorithm	4.5 ms	4.01 ms	3.97 ms

4.6 ATEB-GABOR ALGORITHM AND WAVE THINNING METHOD

We have proposed Ateb-Gabor filtering, and based on filtering, thinning by the wave algorithm. Biometric images can be filtered based on the Ateb-Gabor filter. Such filtering will provide better characteristics than the known Gabor filter [168]. The one-dimensional Gabor filter based on Ateb functions allows to get more flat shapes, so it is possible to implement filtering with a wider range of curves and a larger set of control parameters. In particular, four parameters for the Ateb-Gabor filter are m, n, σ, θ as opposed to two for the previously known Gabor filter – σ, θ.

Filtration of two-dimensional Ateb-Gabor is performed by the formula:

$$ATEB-G\left(x,y,\lambda,\theta,\psi,\sigma,\xi\right)=e^{-\frac{x'^2+\psi xy'^2}{2\sigma^2}Ateb-ca\left(\frac{2\prod x'}{\lambda}+\xi\right)},$$
$$\begin{cases}x'=x\cos(\theta)+y\sin(\theta);\\ y'=-x\sin(\theta)+y\cos(\theta),\end{cases}$$

(4.9)

where λ is the wavelength of the cosine multiplier; θ is the normal orientation of the parallel bands; ξ is the phase shift; ψ is the compression ratio.

It is possible to see that if the parameters m, n are less than one, the filter will have a shape with many «strokes». When m, n is more than one, there are usually two black strokes. The filter is made with the parameter $\sigma=1$, the standard deviation of the Gaussian nucleus.

This avoids noise in the low and mid frequencies. Next, let's use the wave algorithm filtered by Ateb-Gabor [168].

The wave algorithm can be divided into two stages: the stage of construction of the primary graph. It includes the start of the wave, tracking the distance traveled, places of separation and attenuation of the wave. The next stage of graph optimization is the result of which it is rejected.

In the first stage, a spherical wave is launched inside the object. Points belonging to individual wave generations are tracked by the central pixels of each odd generation and placed in the primary graph. The primary graph usually contains a large amount of redundant information, so at the stage of graph optimization, extra points are removed.

In the second stage, the construction of the primary graph is performed. It is carried out by tracking the path of the spherical wave in the image.

A spherical wave is triggered from any pixel inside an object. To obtain the generation of a spherical wave, alternate 4 and 8 connected propagation is used. Connection capabilities are characterized by the number of adjacent pixels for the current pixel. For the 4 connected wave propagations, the upper, lower, right, and left pixels of the current pixel are considered adjacent (**Fig. 4.26, a**). For 8 bound propagations, respectively, all 8 pixels around the current one are considered adjacent (**Fig. 4.26, b**). In **Fig. 4.26** the letter *P* indicates the current pixel, and its neighbors are numbered for 4 and 8 connected views, respectively.
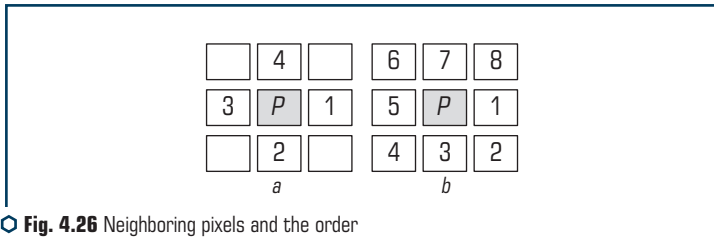

○ **Fig. 4.26** Neighboring pixels and the order of their traversal for: *a* – 4 linked views; *b* – 8 linked views

The spherical wave is characterized by some features:

— no more than $2N$ steps of wave propagation becomes stable, regardless of the initial point of wave propagation, where N is the line width in pixels;

— such a wave well surrounds various obstacles. Small interference of 1–2 pixels has little effect on wave propagation. However, it is better to remove such obstacles at the stage of obtaining a binary image for wave stability.

Zero generation consists of one initial pixel. It affects the image first. The first generation of the wave consists of unnoticed neighbors of the initial pixel with 4 coherent propagation. First generation pixels are marked in red on the image. In **Fig. 4.27** they have numbers 1, 2, 3, 4. The second generation are unnoticed neighbors of the first-generation pixels with 8 connected propagation.
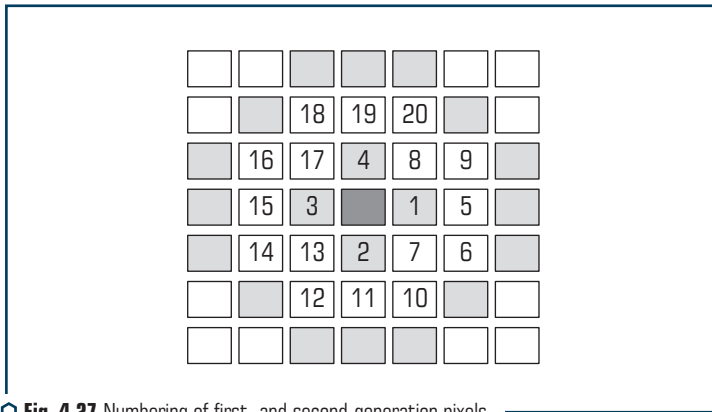

○ **Fig. 4.27** Numbering of first- and second-generation pixels

For each point with coordinates (i, j) it is checked whether its neighboring pixels are marked, it happens in a fixed order – always starting from the right middle pixel clockwise. Then at 4 connected distribution check takes place in the order shown in **Fig. 4.26, *a***, and at 8 connected distribution – as in **Fig. 4.26, *b***. In **Fig. 4.27** it can be seen that the order of the second generation pixels bypass in the example does not correspond to the order of the pixels in the image.

This is due to the fixed order of designation of neighboring pixels, but this simplifies the algorithm [170].

4.7 SOFTWARE FOR SKELETONIZATION

Quality improvement software for skeletonization based on Ateb-Gabor filtration is shown in **Fig. 4.28**. The software consists of the following modules frequest, ridge-freq, ridge-segment, ridge-orient, ridge-filter, image-enhance, main-enhancement.

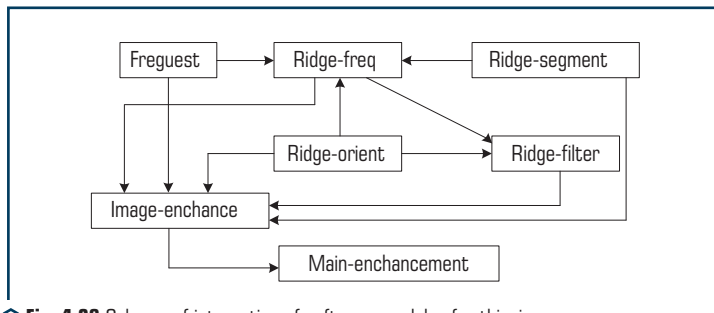The scheme of interaction of modules is shown in **Fig. 4.28**.

○ **Fig. 4.28** Scheme of interaction of software modules for thinning

Improving image quality with orientation filters

The ridge_filter module enhances fingerprint images with targeted filters.

The arguments of the function are: im — image block to be processed; orientim — peak orientation image obtained from ridge_orient; freqim — peak frequency image obtained from ridge_freq; kx, ky — scale factors that determine the sigma of the filter relative to the wavelength of the filter. This is done so that the filter shapes are scale-invariant. kx controls the sigma in the x direction along the filter, and therefore controls the bandwidth of the filter. ky controls the sigma through the filter and therefore controls the orientational selectivity of the filter. A value of 0.5 for both kx and ky is the optimal starting point; showfilter — optional pointer 0/1. When it is specified, the image with the largest filter is displayed for verification.

The function returns: newim — improved image. Rounding the frequency array to the nearest 0.01, to reduce the number of different frequencies you have to deal with.

To establish the reliability of the results, experimental studies were performed on a subset consisting of 955 images of fingerprints NIST-14. The special NIST 24 database [155] is a standard and fully accessible database containing fingerprint images. In a set of turns, the prints are placed at different angles. The set includes the fingers of 10 people, 300 images (from zero to 512×512 pixels) on each finger.

A data set for filtering has been developed in the biometric security system. For this purpose the bank of frequency characteristics of the Ateb-Gabor filter is formed. The classic Gabor filter has 10 frequency characteristics. The study consisted of comparing the results of existing methods of skeletalization with the algorithm developed by the authors of the publication. To study the comparison of results, the Zhang-sung algorithm and the Hilditch's algorithm were used and our own method was developed.

Method of information identification based on Ateb-functions

Basic for graphic information processing systems are two main formats of image representation — raster and vector. Let's consider in comparison raster and vector formats of representation of images and features at recognition.

Digital images in bitmap formats are ordered sequences of strings, which in turn are ordered sequences of pixels. Thus, each pixel is characterized by its value and two coordinates: the line number and the pixel number in this line. Any physical object in a raster image of natural origin is displayed as a set of points of this raster. Because pixels do not contain information about their belonging to a particular object, a certain amount of raster data has to be processed during recognition. This leads to a large increase in processing time. The complexity of raster recognition is also due to the fact that to construct the characteristics of objects that would be resistant to affine transformations of the image, it is extremely difficult.

Vector images are the basis of vector images. Each vector object is characterized by its own numerical, specific geometric, metric, topological and other properties. These are, for example, configuration, structure, location in the image, orientation, and so on. Objects must have metric characteristics, which is achieved by establishing a certain coordinate system and defining metrics [143]. Since all objects are interconnected by one image to which they belong, the coordinate system becomes a common characteristic of this image. In addition to the mentioned properties, vector objects can be associated with data of any nature — numerical, textual, etc. This property of vector objects determines the possibility of created tables and databases for objects that form images. Image recognition in a vector representation has a number of other advantages over bitmap images [171]:

— the ability to group, sort, display, analyze objects by layers;

— gain in the speed of recognition algorithms, which is associated with the possibility of recognition for a small proportion of objects;

— gain in the speed and reliability of recognition due to the grouping of objects by types, which apply to the specific group-specific processing methods, criteria, prototype database, etc.

Solving the problem of information identification on the basis of similarity measures

For the effective functioning of image processing systems requires constant replenishment of the arsenal of methods and tools for pre-processing, image compression and construction of classifiers, which determines the relevance of the development of new tools. Creating effective technologies requires the development of methods and algorithms that must meet a number of requirements for speed and accuracy. The solution of information identification problems is determined by the development of new technologies for processing, analysis and recognition of different types of images.

As a rule, each algorithm, having certain characteristics, «specializes» in its type of image. Recognition of secure documents that contain images in the form of security grids with Ateb functions requires the development of new identification methods that take into account the characteristics of these functions.

The method of skeletonization of the scanned image

To build a skeleton to improve image quality, the image was previously filtered [172]. The filtering process avoids accidental noise in the scanned image.

According to the stages of identification, let's consider in detail the process of skeletonization.

A vector representation of a raster object is a weighted graph with a given mapping. according to the formula (**Fig. 4.10**). For the vertices of the graph let's consider the points of connection

of lines in the raster image. The thickness of the line will be considered the distance between the nearest extreme points of the edge. The graph also shows the display, which takes into account that the image may consist of segments of straight lines. Or, or from arcs of a certain radius (**Fig. 4.10**).

To implement the skeletonization process, it is necessary to convert many pixels of the image object into the appropriate graph. The method is as follows. Based on the image matrix, a graph incidence matrix is constructed using a wave algorithm. Thus, the conversion of a raster image into a vector is realized.

The method of passing a spherical wave in the image

Wave techniques are widely used in computer graphics to determine the minimum distance from one object to another in a limited discrete space. To do this, choose the starting point for the generation of a spherical wave, which propagates according to a certain law in the image. Since space is discrete, the propagation of a spherical wave occurs discrete with the fixation of information at each step. In the current step, the image points reached by the wave are marked. The process ends in a step, provided that the wave reaches a predetermined fixed target point. The step number that marks the target point is the spherical distance from the starting point to the target.

When propagating a wave in a raster image, there are the following limitations: discreteness of space and discreteness of the directions of propagation of a spherical wave (90 degrees for 4 linked rasters, 45 % for 8 linked rasters).

Given these constraints, the wave propagation laws will be different for 4 connected rasters (**Fig. 4.29**) and 8 connected rasters (**Fig. 4.30**). More complex distribution laws are also permissible. At 4-connected raster distribution extends in the form of a diamond, at 8-connected — in the form of a square.

To generate a spherical wave, it is necessary to combine the 4th and 8th connected wave propagation (**Fig. 4.31**). This is achieved by alternately using the 4th and 8th connected propagation. As a result, let's obtain a distribution in the form of an octagon perfectly enveloping the obstacle.

The wave method is to analyze the path of a spherical wave in the image. At each step, the displacement of the center of mass of the points forming the new step of the wave relative to the previous position of the center of mass is analyzed.
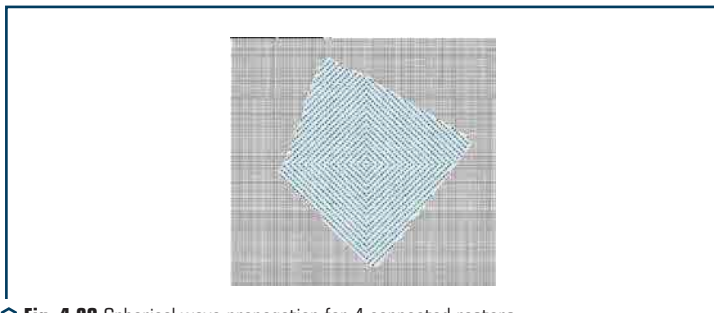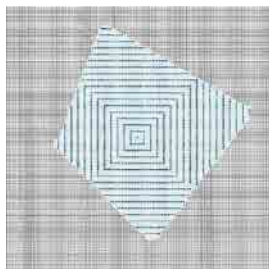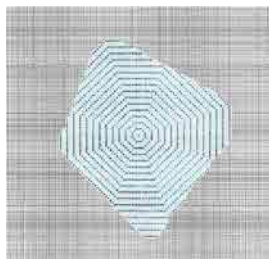

○ **Fig. 4.29** Spherical wave propagation for 4 connected rasters

○ Fig. 4.30 Spherical wave propagation for 8 connected diamond-shaped rasters

○ Fig. 4.31 Spherical wave propagation for 8 connected rasters in the shape of a square

The method consists of the following steps:
1. Building a skeleton of an object using a spherical wave.
2. Optimization of the obtained skeleton.
3. Building the skeleton of an object.
Let's describe in detail the first stage.
Let's consider ways to pass a spherical wave in the image.

4.8 THE METHOD OF PASSING A SPHERICAL WAVE IN THE IMAGE

When propagating a spherical wave on a segment of a straight line no more than in steps, the propagation of the wave will be stable regardless of the starting point, where is the thickness of the straight line in pixels (**Fig. 4.32**).
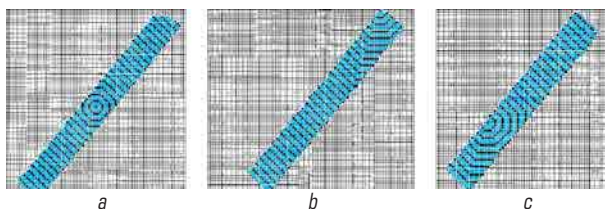
○ **Fig. 4.32** Propagation of a spherical wave for a line segment: *a* – with the starting point in the center of the segment; *b*, *c* – with a starting point at the beginning of the segment

Wave propagation on a curve

The passage of a wave in an arc is well realized by the wave method, because the spherical wave has good enveloping properties (**Fig. 4.33**).
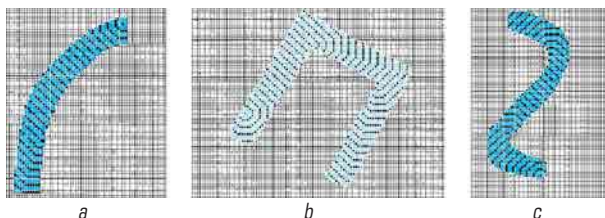

○ **Fig. 4.33** Propagation of a spherical wave along the curve: *a* – skeletonization of the arc; *b* – skeletonization of the broken; *c* – skeletonization of the arc of a more complex shape

Passage of obstacles by a spherical wave

If there are obstacles in the path of a spherical wave, the behavior of the wave depends entirely on the shape and size of the obstacle. An interference of 1–2 pixels has little effect on the propagation of a spherical wave, forming a slight perturbation. Larger obstacles cause significant distortions in the behavior of wave propagation (**Fig. 4.34**).
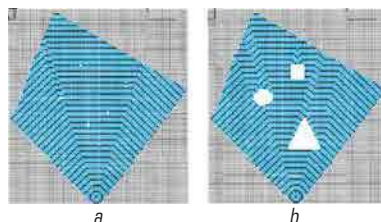

○ **Fig. 4.34** Propagation of a spherical wave with interference in: *a* – 1–2 pixels; *b* – more pixels creates significant interference

Separation of a spherical wave at the intersection of segments

When the spherical wave reaches the point of intersection of the segments, the wave is divided into several daughter waves, which preserve the behavior of the parent wave (**Fig. 4.35**).
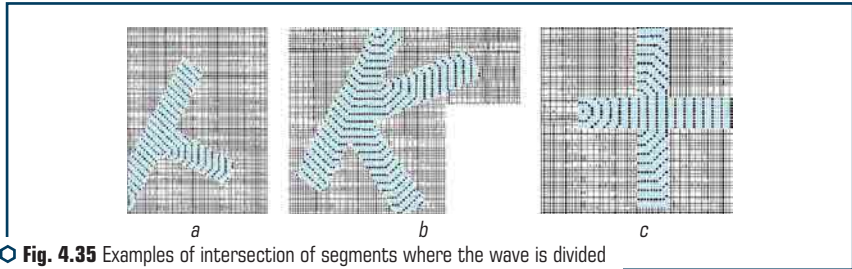

a   *b*   *c*

○ **Fig. 4.35** Examples of intersection of segments where the wave is divided into several daughter waves

The division is easy to trace by analyzing the wavelength, i.e. the number of wave points that form the next generation. Before separation, there is an increase in wavelength, followed by division into two or more daughter waves.

The analysis of the image line is realized by analyzing the movement of the center of the segment formed by the extreme points of wave generation. After the analysis, it is possible to smooth the segment in order to reduce the number of nodal points (**Fig. 4.36**).
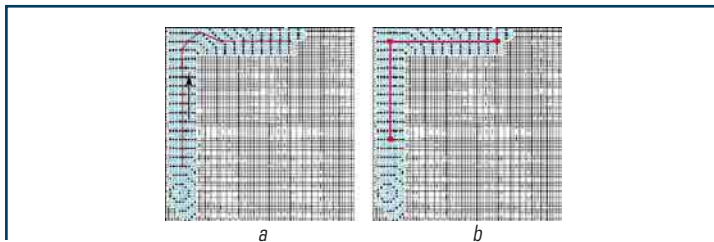

a   *b*

○ **Fig. 4.36** Examples of image line analysis and segment smoothing to reduce the number of nodal points: *a* — segment analysis; *b* — segment optimization

Appointment date

The revealed function of increasing the «width» of the wind and the length of the wind on the daughter allows to set the point of transfer of the two windings. Moreover, to take into account two extreme points *A*, *B*, which are to be passed. After subdivision of wind on two winds, let's take two pairs of points *C*, *D* and *E*, *F*. There are only 6 ways to go through the cold weather in the wild season (**Fig. 4.37–4.39**). For whatever possible options, the point of entry of the segments lies in the middle of the six-piece ABCDEF. Let's put the place on the back as the center of the mass of the polygon. At the stage of optimizing the skeleton of the image, correction is implemented.
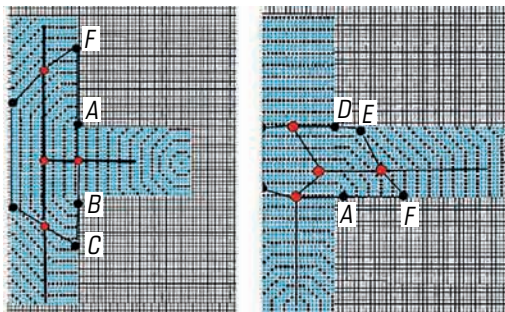
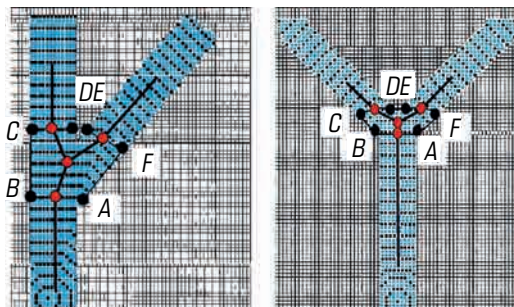**Fig. 4.37** Optimization of the path of the wave passage at an angle of 90°

Fig. 4.38 Ways to get through the bad weather
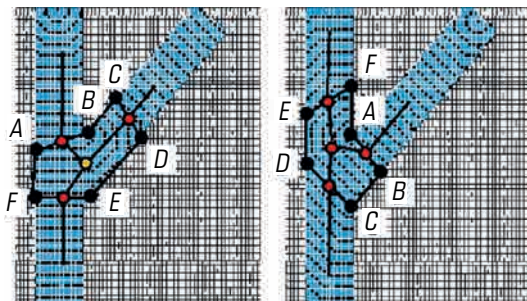

Fig. 4.39 Optimization of the path of wave passage in the case of an obstacle with a sharp angle

Skeleton optimization

Removing the skeleton of the image is not optimal (**Fig. 4.40**).

It is necessary to optimize the skeleton taken at the first stage by analyzing the path of spherical hair on the image of the object. In a limited skeleton, it is possible to represent one in a row with a succession of edges.
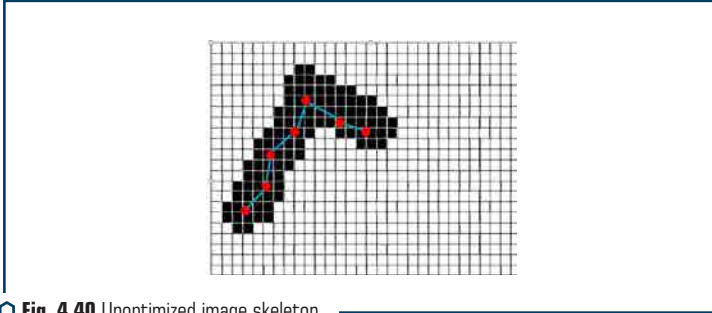
○ **Fig. 4.40** Unoptimized image skeleton

Windage optimization

Contemplations, like calls to the low division of the image building (**Fig. 4.41**) are seen as a path to the analysis of the sequence of ribs. From the given value, lay down the level of optimization: the more allowable input, the less number of points will be included in the resulting graph (**Fig. 4.42**).
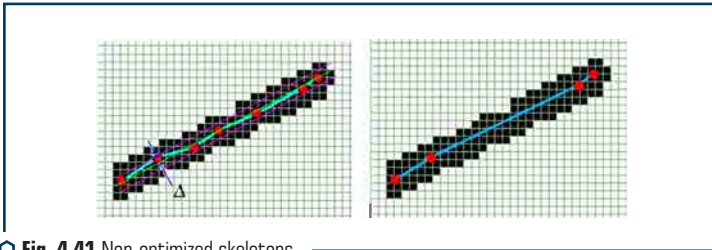

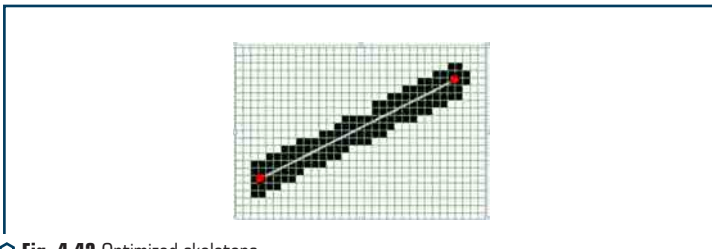○ **Fig. 4.41** Non-optimized skeletons

○ **Fig. 4.42** Optimized skeletons

Airdrop point optimization

For optimizing the skeleton, about the points of connection are analyzed, so that such points are destined to split the wind into two winds.

Most often, there are attempts (**Fig. 4.43, *a***) to correct for additional analysis of adjacent points (A) to AB_1, B_1C_1, AB_1, B_2C_2, AB_3, B_3C_3. The analysis is based on the search for point A′ (point of remembrance), such as A′A, AB_1; A′B_3, B_3C_3; and A′B_2, B_2C_2 correlate as much as possible to a straight line. The graph edges B_3A, B_2A, B_2C_2, B_3C_3 are replaced by the edges A′C_2, A′C_3, A′B_1 (**Fig. 4.43, *b***).

Another variant of distortion is the case of connection of three segments at one point (**Fig. 4.43, *c***). In this case, it is impossible to find a pair of edges that correlate with the line. Then let's construct the point A′ as the center of the triangle formed by the lines B_1C_1, B_2C_2 and B_3C_3. The edges of the graph AB_3, AB_2, AB_1, B_1C_1, B_2C_2, B_3C_3 are replaced by the edges A′C_2, A′C_3, A′C_1 (**Fig. 4.43, *d***).
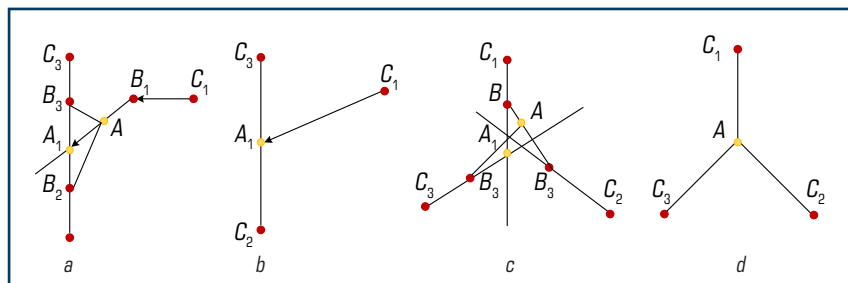

Fig. 4.43 Optimization of the point of entry: *a* – the unoptimized skeleton of the image, the distortion that occurs when the wave is divided into two half-waves; *b* – the optimized curve of the image; *c* – the distorted connection of segments due to the implementation of the wave method; *d* – the optimized version

Algorithm for inducing the skeleton of the image for the help of a spherical hair

The construction of the skeleton is reduced to the selection of segments and their junctions with the entry of the found data in the resulting graph. Selection is performed by analyzing the path of the wave, with the mark of the path traveled (to prevent double passage of the wave in the image). In the resulting graph of the skeleton of the image, the midpoints for skin wrinkle generation are entered. As a result of reducing the number of points in the process of spinning, an analysis of the movement of the middle point of the remaining generation of spins is carried out, and only a few points are entered in the graph, in which a change is made directly to the move of the middle point (**Fig. 4.44, *a***).

To see the edges, points de are assigned:

1) there is a division of the wave into two waves, i.e. the connection or intersection of segments (**Fig. 4.44, *b***);

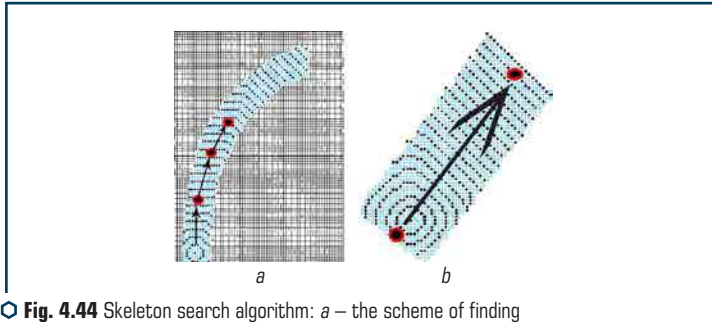2) there is a sign of sickness, so that the wind blows (**Fig. 4.44**).

○ **Fig. 4.44** Skeleton search algorithm: *a* – the scheme of finding
a skeleton along a curve; *b* – an enlarged version of creating a skeleton

In case of extinction, there are two options:

1. The wave reached the end of the rib (**Fig. 4.44**).

2. The wave has reached the point of closing of the ribs (**Fig. 4.44**).

The skeleton search algorithm is recursive. The algorithm will terminate if there is no room for further expansion of the wind.

4.9 METHODS OF SEEING PARTICULAR POINTS ON THE FINGERTIPS

Among the main approaches for recognizing fingers, it is possible to see the sprat, the most common:

– alignment at particular points;

– correlation comparison;

– setting according to the template;

– alignment on the basis of graphs.

On the scanned image of the card, there are also special points, which are aligned with the templates. The main advantage of this algorithm is the speed of its work and ease of implementation. Up to a short distance between the algorithms, according to special points, one could see the high places until the clarity of the image and the vision of the day [173].

The essence of the method of correlational matching lies in the fact that the removal of the number of fingers is superimposed on the skin standard from the data base on the basis, after which the distribution of the differences between them is determined by the pixels. The process of alignment can include impersonal iterations, on the skin of which images are rotated under a small hood, the trochs are shifting. Therefore, this method is the most important and requires a high calculation of pressure.

In the algorithm of setting according to the template, not only just taken points are taken to the point of respect, but also the general characteristics of the finger's stroke, such as

the thickness of smog, its curvature or its sharpness. The advantages of this method are those that can be used with higher quality. But this method is not attached to anonymous searches in the database.

In the method of matching according to the vicarious pattern, the peculiarities of the appearance of the papillary pattern are observed. Obtained image, divided into impersonal other midpoints, in the dermal layer, the lines are described by the parameters of sinusoidal wheezing. The deletion for the equalization of the vouchers is changed and brought to the same mind as the template. The main advantages of the considered algorithm are to reach the high speed and low visibility to the clarity of the image.

In the alignment algorithm based on graphs, the image is transformed into an image of the papillary line orientation field, on which the area is shown with the same orientation of the lines. Then the centers of the regions are appointed and the graph comes out. The next steps are similar to the method of alignment at singular points.

Exploring the method of matching the fingertips

Pairing of finger marks is based on the search for specific points on images, search for specific reference points on images, the assigned value of attributes of specific points on images. At the result, let's accept the decision that the images are identical, as if the images could have a single multiple M of the same distinct singular points.

The rule may be applied to new data, which will be entered into the system, and the number of different pairs of dots is smaller than the two higher numbers of special dots on the images. That is why to mark the summation of special points of the first image with the most significant points of the other image. Subsequently, by matching their reference points and correspondingly rotating the special points of one of the images around the reference point in this image, calculate the total number of special points of the two compared images in the overlap of these images and decide that the two compared images are identical, based on the number of found corresponding points, as well as large numbers of singular points in the region of overlap between the two images [174].

There is a way that two images, as if they are aligned, with the help of one finger, counting the world of the proximity of these images for the formula:

$$sim = identical / \sqrt{(k\_1 \cdot k\_2)}, \tag{4.10}$$

where identical k_1, k_2 – the number of known points and the highest number of singular points of two images in the region of their overlap, that comparise calculated the world of proximity to the previously given boundary values.

It can be said that the images are identical, as if their reference points on two identical images are from the number of special points, as if they correspond to the points or to the lines of the papillary lines.

Searching for singular points can also be searched for by searching for multiples of M pairs of distinct points along the path of a continuous bipartite graph, the left and right vertices of

which indicate the singularities of the points of the first and the other paired images, and the arcs of the graph – the sum of the names of the differences, the arc of the attribute This is the importance of the optimal marking of the vertices of the i-th bipartite graph [175].

It is also possible to designate a plot of overlapping two images, as if they were equal, as such, that overlapping swollen shells of many special points on these images.

○ **Fig. 4.45** The butt of the identification of special points of the finger

From taking a point at the forward stages, an array of objects is formed with the following parameters: point coordinates; line type; satisfactions with them. Set parameters for specific points, subtracting from the scanned finger, compare with the set of reference parameters for user registrations RU. At the next stage, the values of these parameters are determined. The great threshold of improvement is to improve the ability to change the biometric characteristics of two users – FAR (False Acceptance Rate). On the other hand, a small value of allowable resignation is the reason for the increase in the ability to move and the legal user RU – FRR (False Rejection Rate). The problem of choosing the tolerance threshold is due to the deformation of that misplaced finger during scanning, which leads to the elimination of different parameters of the selected points. As a result of the research, it was established that it was possible to collect additional information about the combination of three special points. Such a structure, called a triplet, is shown in **Fig. 4.46**.
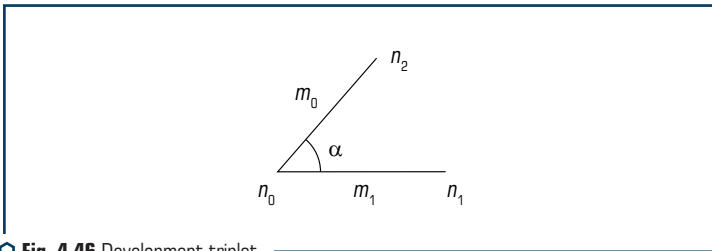

○ **Fig. 4.46** Development triplet

For the skin central point $n_0(xn_0, yn_0)$ and two suicidal points $n_1(xn_1, yn_1)$ and $n_2(xn_2, yn_2)$ a vector of parameters is formed.
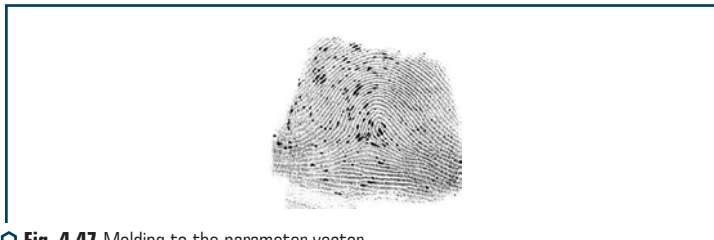
○ **Fig. 4.47** Molding to the parameter vector

The algorithm shows the procedure for training the mask for the skin pair of the browser. Let's accept a rude joke: which one is the most effective, but the most effective and the most effective. Through a small expansion of the initial data, it is possible to see that brute force is possible and gives the best result. So, first of all, redistribute the skin pair of the browser (row 1), and then it is possible to use masks (row 4). For a skin mask, let's review the description (row 7) and reconsider which mask was chosen to improve stability across browsers, multiplying uniqueness (row 8–11 and 14–17).

Let's generate a finger bitcoin on the server side based on hashes on the client side of the date. As it was already guessed, the finger hit is a hash, which is calculated from the «i» operation of the hash list of all tasks and a mask. Mask – just for one browser fingerprinting, and counted for two submasks for cross browser fingerprints.

Generation of a mask for two skin browsers is the training course. In particular, let's use a small subset to obtain a mask that optimizes both stability between browsers and creates uniqueness.

Comparison of selected special points with the help of machine learning

There is a finite number of data – a training sample. Each element is described by a set of features x («feature vector»). For each vector of parameters x the answer y is known.
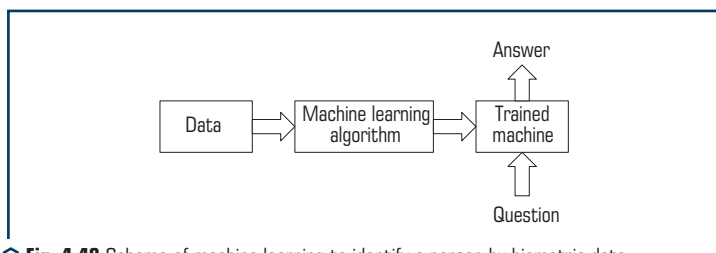
○ **Fig. 4.48** Scheme of machine learning to identify a person by biometric data

The problem of machine learning is that it is necessary to construct a function $y = f(x)$ from the vector of signs x, which gives the answer y for any possible observation x.

Ateb-Gabor filtration and selection of special points

The Ateb-Gabor filter is a product of the Gaussian and periodic Ateb function, which improves the monotonic areas of periodic images. In the case of fingerprints, it is assumed that the

periodicity of the lines and the standard deviation are consistent mainly with the local characteristics of the image. Ateb-Gabor filters give a strong reaction at those points of the image where there is a component with local features of frequency in space and orientation [176].

Ateb-Gabor two-dimensional filter is used for image filtering. It is a harmonic function multiplied by the Gaussian function. The two-dimensional Ateb-Gabor filter has the form shown in (4.9).

In this equation λ is the wavelength of the cosine multiplier, θ is in degrees, ψ is the phase shift in degrees, and φ is the compression ratio, m, n are the parameters of the Ateb function, 2 is the period of the Ateb-function [146].

An experiment was performed with Ateb-Gabor and Gabor filtering of fingerprints based on the freely available NIST Special Database 302. The results of experiments showed that as a result of correlation, images change significantly, the higher the values of *m*, *n*, σ are laid [162].

Physical access to the identification system

The computer is connected directly from the Arduino Nano via a USB adapter (**Fig. 4.50**).

An important point is to connect the fingerprint scanner to the Arduino Nano. **Fig. 4.50** makes it difficult to understand how cables are connected to their ports, so **Fig. 4.51** shows a schematic diagram of a scanner connection.

The DY50/AS608 fingerprint sensor has 6 wires. If to look at the back of the sensor from left to right, they are marked as follows: T-3V3 – leave unconnected; T-OUT – leave unconnected; 3V3 – to the Arduino 3V3 port; TX – to the Arduino port D2; RX – to the Arduino port D3; GND – to the Arduino GND port.
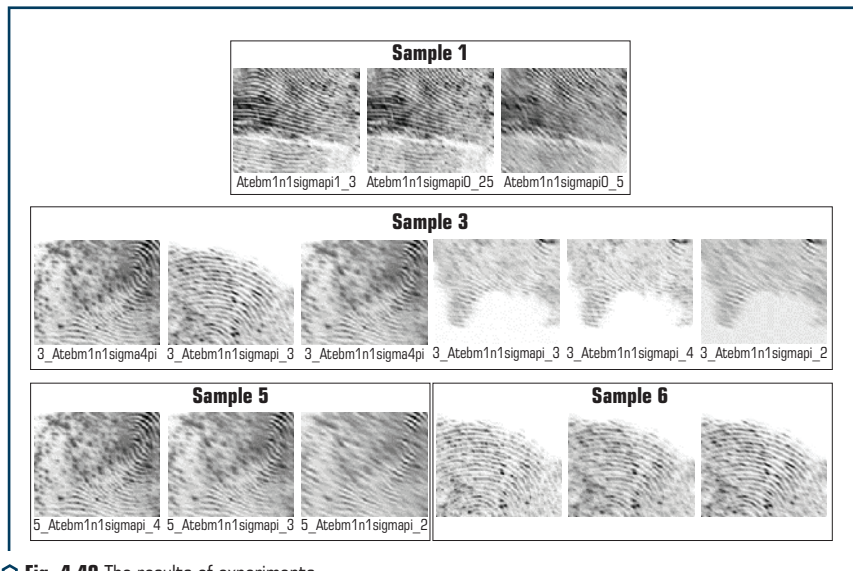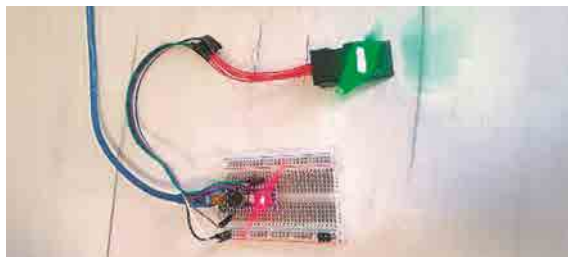

Fig. 4.49 The results of experiments

○ Fig. 4.50 Image of the fingerprint scanning and analysis system
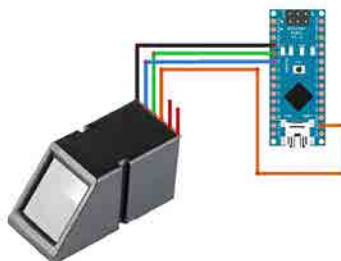
○ Fig. 4.51 Fingerprint scanner connection diagram

To demonstrate the operation of the fingerprint verification system using intelligent analysis, two firmwares have been created for the system.

1. Custom firmware – which searches the fingerprint database and searches for the corresponding user fingerprint.

The firmware itself is quite simple. It has made it much easier to write code with the Fingerprint Library. «Confidence» is the number of points (from 0 to 255), which indicates how well the fingerprint matches, the more the better. It is possible to notice that if it matches at all, it means that the sensor is quite reliable, so do not need to pay attention to the trust number, if it does not make sense for programs with a high level of security. Of course, it is necessary to register a fingerprint first. It is necessary to download the administrator firmware to register your fingerprints.

2. Firmware with administrator rights – allows to work with the database and perform a search. Enroll allows to add fingerprints to a database under one of the indexes, the number of indexes is limited by the maximum amount of scanner memory (127 templates). The program allows to choose under which ID let's save your fingerprint (**Fig. 4.51**), then run the script to read the fingerprint.

This subroutine is responsible for the function getFingerprintEnroll (more in the appendix) to add fingerprints, schematically it is written as follows, it is described as follows:

— the detector works similarly to custom firmware, the reason for integrating into the administrator's firmware is the ability to test in real time changes in code and bugs, also to check whether the fingerprint will be read;

— the algorithm check performs the same function as adding a fingerprint. The only difference is that the fingerprint template recorded in the database has already been processed and saved in the image format of the fingerprint skeleton. That is, the read fingerprint is first pre-processed, and only then compared with those present in the database.

CONCLUSIONS

1. The development of computing resources, quantum computers and the rapid growth in the use of wireless and mobile technologies allow the formation and development of smart technologies, new network formats based on their synthesis with classical networks. However, in pursuit of super speeds and digitalization, developers do not pay due attention to the security of such systems. The formation of socio-cyber-physical systems based on the integration of cyberspace with smart technologies forms unprotected hybrid systems. In a full-scale quantum computer, this approach exacerbates the ability to provide the required level of security. In addition, the use of cloud technologies requires a reassessment of approaches to the formation of a security system. The proposed Concept provides the basis for the formation of security systems in the post-quantum period and provides a fundamentally new approach to the objectivity of assessing cyber threats. In addition, not only the signs of threats such as synergy and hybridity are taken into account, but also the integration and globalization of technologies, as well as the form of ownership, which can technically and materially affect the final elements of the socio-cyber-physical systems infrastructure.

2. The study performed a theoretical summary and proposed a new solution to the urgent scientific and applied problem: creating methodological foundations to build a system of information security in social networking services. It uses new methods to identify, assess and counteract threats to the information security of the state in the information space. As a result of the performed research, the approaches to the formation of the system of information security in the conditions of globalization and free circulation of information acquired further development in the sphere of information security of the state. The lack of similar solutions makes the results of research a priority. The obtained scientific results have a fundamental theoretical and applied practical importance for ensuring information security of the state in the social networking services and contribute to the further development of modern information technologies that implement security functions.

3. Problems of physical access to critical infrastructure for biometric information protection systems have been developed. The theory of pre-processing of data on filtering of biometric images is developed. A system of biometric protection has been built, which works on the basis of comparison of biometric prints and reveals similarities with a certain template, which is stored in a biometric database. The stage of skeletonization is developed and the wave algorithm of thinning which is realized after Ateb-filtration is offered. The propagation of the wave on the curve is considered in detail. Software for skeletonization based on Ateb-Gabor filtration has been developed. A two-dimensional Ateb-Gabor filter is used for image filtering. It is a harmonic function multiplied by the Gaussian function. The intellectual analysis of data of comparison of the scanned fingerprint with a template by the k-means method is carried out. Good puncturing characteristics are reached. Experiments of biometric prints based on NIST-14 showed the effectiveness of the proposed method. An experimental stand was implemented, where the connection to the computer is made directly from the Arduino Nano.

REFERENCES

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: http://doi.org/10.15587/978-617-7319-31-2

2. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et. al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. doi: http://doi.org/10.15587/1729-4061.2021.233533

3. Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. International Affairs, 92 (5), 1079–1105. doi: http://doi.org/10.1111/1468-2346.12706

4. Konstantas, J. (2016). Dam Hackers! The Rising Risks to ICS and SCADA Environments. Security Week. Available at: http://www.securityweek.com/dam-hackers-rising-risks-ics-and-scada-environments

5. Westervelt, R. (2012). Old Application Vulnerabilities, Misconfigurations Continue to Haunt. TechTarget. Available at: http://searchsecurity.techtarget.com/feature/Old-Application-Vulnerabilities-Misconfigurations-Continue-to-Haunt

6. Ashford, W. (2014). Industrial control systems: What are the security challenges? Computer Weekly. Available at: http://www.computerweekly.com/news/2240232680/Industrial-control-systems-What-are-the-security-challenges

7. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et. al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105), 6–19. doi: https://doi.org/10.15587/1729-4061.2020.205702

8. Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems. Vienna: Premier Publishing s. r. o. doi: http://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018

9. Kondratov S., Bobro D., Horbulin V. et. al.; Sukhodolia, O. (2017). Developing The Critical Infrastructure Protection System in Ukraine. Kyiv: NISS.

10. Rinaldi, S. M., Peerenboom, J. P., Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies. IEEE Control Systems Magazine, 21 (6), 11–25. doi: http://doi.org/10.1109/37.969131

11. Casalicchio, E., Galli, E., Tucci, S.; Setola, R.., Geretshuber, S. (Eds.) (2009). Modeling and Simulation of Complex Interdependent Systems: A Federated Agent-Based Approach. CRITIS 2008. LNCS. Heidelberg: Springer, 5508, 72–83. doi: http://doi.org/10.1007/978-3-642-03552-4_7

12. Haimes, Y. Y., Jiang, P. (2001). Leontief-Based Model of Risk in Complex Interconnected Infrastructures. Journal of Infrastructure Systems, 7 (1), 1–12. doi: http://doi.org/10.1061/(asce)1076-0342(2001)7:1(1)

13. Barker, K., Santos, J. R. (2010). Measuring the efficacy of inventory with a dynamic in-put-output model. International Journal of Production Economics, 126 (1), 130–143. doi: http://doi.org/10.1016/j.ijpe.2009.08.011

14. Santos, J. R. (2008). Interdependency analysis with multiple probabilistic sector inputs. Journal of Industrial & Management Optimization, 4 (3), 489–510. doi: http://doi.org/10.3934/jimo.2008.4.489

15. Jung, J. (2009). Probabilistic Extension to the Inoperability Input-Output Model: P-IIM. Charlottesville.

16. Santos, J. R., Haimes, Y. Y., Lian, C. (2007). A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies. Risk Analysis, 27 (5), 1283–1297. doi: http://doi.org/10.1111/j.1539-6924.2007.00957.x

17. Nieuwenhuijs, A., Luiijf, E., Klaver, M.; Papa, M., Shenoi, S. (Eds.) (2008). Modeling Dependencies Critical Infrastructures. Critical Infrastructure Protection II: Proceedings of the Second Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection. IFIP. Springer, Heidelberg, 290, 205–213. doi: http://doi.org/10.1007/978-0-387-88523-0

18. Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., Porcellinis, S. D., Setola, R. (2008). Modelling interdependent infrastructures using interacting dynamical models. International Journal of Critical Infrastructures, 4 (1/2), 63–79. doi: http://doi.org/10.1504/ijcis.2008.016092

19. Panzieri, S., Setola, R. (2008). Failures propagation in critical interdependent infrastructures. International Journal of Modelling, Identification and Control, 3 (1), 69–78. doi: http://doi.org/10.1504/ijmic.2008.018186

20. Rinaldi, S. M. (2004). Modeling and Simulating Critical Infrastructures and Their Interdependencies. Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS 2004). IEEE Computer Society Press, Big Island. doi: http://doi.org/10.1109/hicss.2004.1265180

21. Forrester, J. W. (1961). Industrial Dynamics. Waltham: Pegasus Communications.

22. Forrester, J. W. (1961). Principles of Systems. Waltham: Pegasus Communications.

23. Gonzalez, J. J., Sarriegi, J. M., Gurrutxaga, A.; Lopez, J. (Ed.) (2006). A Framework for Conceptualizing Social Engineering Attacks. CRITIS 2006. LNCS, vol. Heidelberg: Springer, 4347, 79–90. doi: http://doi.org/10.1007/11962977_7

24. Bier, V. M., Ferson, S., Haimes, Y. Y., Lambert, J. H., Small, M. J. (2004). Risk of Extreme and Rare Events: Lessons from a Selection of Approaches. Risk Analysis and Society: An Interdisciplinary Characterization of the Field. Cambridge: Cambridge University Press, 74–118. doi: http://doi.org/10.1017/cbo9780511814662.004

25. Bier, V. M. (2001). Game Theoretic Models for Critical Infrastructure Protection. Abstracts of the 2001 Society for Risk Analysis Annual Meeting «Risk Analysis in an Interconnected World».

26. Von Neumann, J., Morgenstern, O. (1947). Theory of Games and Economic Behavior. Princeton: Princeton University Press.

27. Burke, D. A. (1999). Towards a Game Theory Model of Information Warfare. Air Force Institute of Technology, Wright-Patterson Air Force Base, 117.

28. Liu, D., Wang, X., Camp, J. (2008). Game-theoretic modeling and analysis of insider threats. International Journal of Critical Infrastructure Protection, 1, 75–80. doi: http://doi.org/10.1016/j.ijcip.2008.08.001

29. Jenelius, E., Westin, J., Holmgren, Å. J. (2010). Critical infrastructure protection under imperfect attacker perception. International Journal of Critical Infrastructure Protection, 3 (1), 16–26. doi: http://doi.org/10.1016/j.ijcip.2009.10.002

30. Yoshida, M., Kobayashi, K. (2010). Disclosure Strategies for Critical Infrastructure against Terror Attacks. Proceedings of the 2010 IEEE International Conference on Systems Man and Cybernetics (SMC 2010). Istanbul: IEEE Press, 3194–3199. doi: http://doi.org/10.1109/icsmc.2010.5642277

31. Major, J. A. (2002). Advanced Techniques for Modeling Terrorism Risk. The Journal of Risk Finance, 4 (1), 15–24. doi: http://doi.org/10.1108/eb022950

32. Lakdawalla, D. N., Zanjani, G. (2004). Insurance, Self-Protection, and the Economics of Terrorism. Tech. Rep. WR-171-ICJ, RAND Corporation. Santa Monica.

33. Woo, G. (2002). Quantitative Terrorism Risk Assessment. The Journal of Risk Finance, 4 (1), 7–14. doi: http://doi.org/10.1108/eb022949

34. Bier, V., Oliveros, S., Samuelson, L. (2007). Choosing What to Protect: Strategic Defensive Allocation against an Unknown Attacker. Journal of Public Economic Theory, 9 (4), 563–587. doi: http://doi.org/10.1111/j.1467-9779.2007.00320.x

35. Sandler, T., Siqueira, K. (2008). Games and Terrorism. Simulation & Gaming, 40 (2), 164–192. doi: http://doi.org/10.1177/1046878108314772

36. Bollobás, B. (1998). Modern Graph Theory. Graduate Texts in Mathematics, Vol. 184. Berlin: Springer.

37. Bollobás, B., Kozma, R., Miklós, D. (Eds.) (2009). Handbook of Large-Scale Random Networks. Bolyai Society Mathematical Studies, 18. János Bolyai Mathematical Society and Springer. Budapest.

38. Albert, R., Barabási, A. L. (1999). Emergence of Scaling in Random Networks. Science, 286 (5439), 509–512. doi: http://doi.org/10.1126/science.286.5439.509

39. Albert, R., Barabási, A. L. (2002). Statistical Mechanics of Complex Networks. Reviews of Modern Physics 74 (1), 47–97. doi: http://doi.org/10.1103/revmodphys.74.47

40. Newman, M. E. J. (2003). The Structure and Function of Complex Networks. SIAM Review, 45 (2), 167–256. doi: http://doi.org/10.1137/s003614450342480

41. Newman, M., Barabási, A. L., Watts, D. J. (Eds.) (2006). The Structure and Dynamics of Networks. Princeton Studies in Complexity. Princeton: Princeton University Press.

42. North, M.; Sallach, D., Wolsko, T. (Eds.) (2000). Agent-Based Modeling of Complex Infrastructures. In: Proceedings of the Workshop on Simulation of Social Agents: Architectures and Institutions. University of Chicago and Argonne National Laboratory, Chicago. ANL/DIS/TM-60, 239–250.

43. Zhu, G.-Y., Henson, M. A., Megan, L. (2001). Dynamic modeling and linear model predictive control of gas pipeline networks. Journal of Process Control, 11 (2), 129–148. doi: http://doi.org/10.1016/s0959-1524(00)00044-5

44. Han, Z. Y., Weng, W. G. (2010). An integrated quantitative risk analysis method for natural gas pipeline network. Journal of Loss Prevention in the Process Industries, 23 (3), 428–436. doi: http://doi.org/10.1016/j.jlp.2010.02.003

45. Wolthusen, S. D. (2005). GIS-based Command and Control Infrastructure for Critical Infrastructure Protection. Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), 40–47. doi: http://doi.org/10.1109/iwcip.2005.12

46. Patterson, S. A., Apostolakis, G. E. (2007). Identification of Critical Locations Across Multiple Infrastructures for Terrorist Actions. Reliability Engineering & System Safety, 92 (9), 1183–1203. doi: http://doi.org/10.1016/j.ress.2006.08.004

47. Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I. et. al. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka-Volterra model. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 30–47. doi: http://doi.org/10.15587/1729-4061.2021.241638

48. Lippert, K. J., Cloutier, R. (2021). Cyberspace: A Digital Ecosystem. Systems, 9 (3), 48. doi: http://doi.org/10.3390/systems9030048

49. Mazurczyk, W., Drobniak, S., Moore, S. Towards a Systematic View on Cybersecurity Ecology. Available at: https://arxiv.org/ftp/arxiv/papers/1505/1505.04207.pdf Last accessed: 25.06.2021

50. Gorman, S. P., Kulkarni, R. G., Schintler, L. A., Stough, R. R. (2004). A Predator Prey Approach to the Network Structure of Cyberspace. Available at: https://www.researchgate.net/publication/255679706_A_predator_prey_approach_to_the_network_structure_of_cyberspace Last accessed: 25.06.2021

51. Ya dogonyayu, ty ubegayesh'. Chto takoye model' Lotki-Vol'terry i kak ona pomogayet biologam. Available at: https://nplus1.ru/material/2019/12/04/lotka-volterra-model

52. Tøndel, I. A., Cruzes, D. S., Jaatun, M. G., Sindre, G. (2022). Influencing the security prioritisation of an agile software development project. Computers & Security, 118, 102744. doi: http://doi.org/10.1016/j.cose.2022.102744

53. Șcheau, M.-C., Leu, M.-D., Udroiu, C. (2022). At the Intersection of Interests and Objectives in Cybersecurity. Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3), 29–34. doi: http://doi.org/10.19107/cybercon.2022.03

54. Mohammed, N. Q., Amir, A., Salih, M. H., Ahmad, B. (2022). Design and Implementation of True Parallelism Quad-Engine Cybersecurity Architecture on FPGA. International Journal of Advanced Computer Science and Applications, 13 (1), 719–724. doi: http://doi.org/10.14569/ijacsa.2022.0130183

55. Nevliudov, I., Yevsieiev, V., Maksymova, S., Filippenko, I. (2020). Development of an architectural-logical model to automate the management of the process of creating complex cyberphysical industrial systems. Eastern-European Journal of Enterprise Technologies, 4 (3 (106)), 44–52. doi: http://doi.org/10.15587/1729-4061.2020.210761

56. Szymanski, T. H. (2022). The «Cyber Security via Determinism» Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). IEEE Access, 10, 45893–45930. doi: http://doi.org/10.1109/access.2022.3169137

57. De Kinderen, S., Kaczmarek-Heß, M., Hacks, S. (2022). Towards Cybersecurity by Design: A multi-level reference model for requirements-driven smart grid cybersecurity. ECIS 2022 Research Papers. 89. Available at: https://aisel.aisnet.org/ecis2022_rp/89/

58. Do Thu, H., Hoang, N. X., Hoang N. V., Du, N. H., Huong, T. T., Phuc Tran, K. (2022). Explainable Anomaly Detection for Industrial Control System Cybersecurity. Available at: https://www.researchgate.net/publication/360383589_Explainable_Anomaly_Detection_for_Industrial_Control_System_Cybersecurity

59. KNX Technical Manual 2CKA001473B8668. (2017). KNX Technical Manual. Busch-Presence detector KNX/Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 198.

60. ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual (2016). Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 648.

61. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O. et. al. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 44–59. doi: http://doi.org/10.15587/1729-4061.2022.254545

62. Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. Nature, 489 (7415), 295–298. doi: http://doi.org/10.1038/nature11421

63. Parthasarathy, S., Ruan, Y., Satuluri, V. (2011). Community Discovery in Social Networks: Applications, Methods and Emerging Trends. Social Network Data Analytics, 79–113. doi: http://doi.org/10.1007/978-1-4419-8462-3_4

64. Madirolas, G., de Polavieja, G. G. (2015). Improving Collective Estimations Using Resistance to Social Influence. PLOS Computational Biology, 11 (11), e1004594. doi: http://doi.org/10.1371/journal.pcbi.1004594

65. Sun, J., Tang, J. (2011). A survey of models and algorithms for social influence analysis Social Network Data Analytics, 177–214. doi: http://doi.org/10.1007/978-1-4419-8462-3_7

66. Anagnostopoulos, A., Kumar, R., Mahdian, M. (2008). Influence and correlation in social networks. In Proceeding of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'08), 7–15. doi: http://doi.org/10.1145/1401890.1401897

67. Goyal, A., Bonchi, F., Lakshmanan, L. V. (2010). Learning influence probabilities in social networks. In Proceedings of the 3st ACM International Conference on Web Search and Data Mining (WSDM'10), 207–217. doi: http://doi.org/10.1145/1718487.1718518

68. Xiang, R., Neville, J., Rogati, M. (2010). Modeling relationship strength in online social networks. In Proceeding of the 19th international conference on World Wide Web (WWW'10), 981–990. doi: http://doi.org/10.1145/1772690.1772790

69. Scripps, J., Tan, P.-N., Esfahanian, A.-H. (2009). Measuring the effects of preprocessing decisions and network forces in dynamic network analysis. In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'09), 747–756. doi: http://doi.org/10.1145/1557019.1557102

70. Tang, L., Liu, H. (2009). Relational learning via latent social dimensions. In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'09), 817–826. doi: http://doi.org/10.1145/1557019.1557109

71. Horovyi, V. M., Onyshchenko, O. S., Polovynchak, Yu. M., Horova, S. V., Kostenko, L. Y., Matviichuk, A. V. et. al. (2015). Tekhnolohii rozvytku i zakhystu natsionalnoho informatsiinoho prostoru. Kyiv: NBUV, 296.

72. Konakh, V. K. (2014). Natsionalnyi informatsiinyi prostir Ukrainy: problemy formuvannia ta derzhavnoho rehuliuvannia. Kyiv: NISD.

73. Onyshchenko, O. S., Horovyi, V. M., Popyk, V. I. (2014). Sotsialni merezhi yak instrument vzaiemovplyvu vlady ta hromadianskoho suspilstva. Kyiv: NAN Ukrainy, Nats. b-ka Ukrainy im. V. I. Vernadskoho, 260.

74. Danik, Yu., Hryshchuk, R., Samchyshyn, O. (2015). Mobile social Internet services as the modern mass communication. Ukrainian Scientific Journal of Information Security, 21 (1), 16–20.

75. Peleshchyshyn, A. M., Sierov, Yu. O., Berezko, O. L., Peleshchyshyn. O. P., Tymovchak-Maksymets, O. Yu., Markovets, O. V. (2012). Protsesy upravlinnia interaktyvnymy sotsialnymy komunikatsiiamy v umovakh rozvytku informatsiinoho suspilstva. Lviv, Vyd-vo Lviv. Politekhniky, 368.

76. Hryshchuk, R. V., Danyk, Yu. H. (2016). Osnovy kibernetychnoi bezpeky. Zhytomyr: ZhNAEU, 636.

77. Hryshchuk, R. V., Molodetska-Hrynchuk, K. V. (2017). Postanovka problemy zabezpechennia informatsiinoi bezpeky derzhavy u sotsialnykh internet-servisakh. Suchasnyi zakhyst informatsii, 3 (31), 86–96.

78. Tufekci, Z., Wilson, C. (2012). Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square. Journal of Communication, 62 (2), 363–379. doi: http://doi.org/10.1111/j.1460-2466.2012.01629.x

79. Savanevskyi, M. (2013). #ievromaidan: ukrainska tsyfrova revoliutsiia ta ostannii shans analohovym politykam staty tsyfrovymy. Watcher. Available at: http://watcher.com.ua/2013/11/29/yevromaydan-ukrayinska-tsyfrova-revolyutsiya-ta-ostanniy-shans-analohovym-politykam-staty-tsyfrovymy/

80. Barovska, A. (2016). Informatsiini vyklyky hibrydnoi viiny: kontent, kanaly, mekhanizmy protydii. Kyiv: NISD, 109.

81. Holloway, M. (2017). How Russia weaponized social media in the Crimea. Realcleardefense.com. Available at: https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_111352.html

82. Perry, B. (2015). Non-linear warfare in Ukraine: the critical role of information operations and special operations. Small Wars Journal, 11 (1). Available at: http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera

83. Obzor sotsyalnykh setei. Leto, 2016 (2016). Slideshare. Available at: https://www.slideshare.net/adproisobar/2016-64479518

84. Pro zastosuvannia personalnykh spetsialnykh ekonomichnykh ta inshykh obmezhuvalnykh zakhodiv (sanktsii) (2017). Ukaz Prezydenta Ukrainy No. 133/2017. Available at: http://www.president.gov.ua/documents/1332017-21850

85. Hryshchuk, R., Molodetska-Hrynhchuk, K. (2018). Methodological Foundation of State's Information Security in Social Networking Services in Conditions of Hybrid War. Information & Security: An International Journal, 41, 61–79. doi: http://doi.org/10.11610/isij.4105

86. Molodetska-Hrynchuk, K. (2017). Outreaches content tracing technique for social networking services. Radio electronics, Computer Science, Control, 2 (41), 117–126. doi: http://doi.org/10.15588/1607-3274-2017-2-13

87. Manning, Chr., Raghavan, P., Schütze, H. (2008). Introduction to Information Retrieval. Cambridge University Press. doi: http://doi.org/10.1017/cbo9780511809071

88. Wardle, C., Derakhshan, H. (2017). Information disorder: toward an interdisciplinary framework for research and policy making. Available at: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

89. Barabash, O. V., Hryshchuk, R. V., Molodetska-Hrynchuk, K. V. (2018). Identification threats to the state information security in the text content of social networking services. Science-Based Technologies, 38 (2), 232–239. doi: http://doi.org/10.18372/2310-5461.38.12855

90. Pennacchiotti, M., Popescu, A.-M. (2011). Democrats, republicans and starbucks afficionados. Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining – KDD'11. doi: http://doi.org/10.1145/2020408.2020477

91. Beller, C., Knowles, R., Harman, C., Bergsma, S., Mitchell, M., Van Durme, B. (2014). I'm a Belieber: social roles via self-identification and conceptual attributes. Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics, 181–186. doi: http://doi.org/10.3115/v1/p14-2030

92. Schwartz, H. A., Eichstaedt, J. C., Kern, M. L., Dziurzynski, L., Ramones, S. M., Agrawal, M. et. al. (2013). Personality, Gender, and Age in the Language of Social Media: The Open-Vocabulary Approach. PLoS ONE, 8 (9), e73791. doi: http://doi.org/10.1371/journal.pone.0073791

93. Gore, R. J., Diallo, S., Padilla, J. (2015). You Are What You Tweet: Connecting the Geographic Variation in America's Obesity Rate to Twitter Content. PLOS ONE, 10 (9), e0133505. doi: http://doi.org/10.1371/journal.pone.0133505

94. Molodetska, K., Tymonin, Y. (2019). System-dynamic models of destructive informational influence in social networking services. International Journal of 3D Printing Technologies and Digital Industry, 3 (2), 137–146.

95. Pasca, M. (2007). What you seek is what you get: Extraction of class attributes from query logs. Proceedings of IJCAI.

96. Faraz, A. (2016). A Comparison of Text Categorization Methods. International Journal on Natural Language Computing, 5 (1), 31–44. doi: http://doi.org/10.5121/ijnlc.2016.5103

97. Fernández-Martínez, F., Zablotskaya, K., Minker, W. (2012). Text categorization methods for automatic estimation of verbal intelligence. Expert Systems with Applications, 39 (10), 9807–9820. doi: http://doi.org/10.1016/j.eswa.2012.02.173

98. Natekin, A., Knoll, A. (2013). Gradient boosting machines, a tutorial. Frontiers in Neurorobotics, 7 (21), 1–21. doi: http://doi.org/10.3389/fnbot.2013.00021

99. Freund, Y., Schapire, R. E. (1997). A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting. Journal of Computer and System Sciences, 55 (1), 119–139. doi: http://doi.org/10.1006/jcss.1997.1504

100. «MIB Datasets» (2017). Mib.projects.iit.cnr.it. Available at: http://mib.projects.iit.cnr.it/dataset.html

101. Hryshchuk, R. V., Mamariev, V. M., Molodetska-Hrynchuk K. V. (2017). Klasyfikatsiia profiliv informatsiinoi bezpeky aktoriv v sotsialnykh internet-servisakh (na prykladi mikroblohu Twitter). Informatsiini tekhnolohii ta kompiuterna inzheneriia, 2, 12–19.

102. Cresci, S., Pietro, R. Di, Petrocchi, M., Spognardi, A., Tesconi, M. (2015). Fame for sale: efficient detection of fake Twitter followers. Decision Support Systems, 80, 56–71. doi: http://doi.org/10.48550/arXiv.1509.04098

103. Milan, S. (2015). From social movements to cloud protesting: the evolution of collective identity. Information, Communication & Society, 18 (8), 887–900. doi: http://doi.org/10.1080/1369118x.2015.1043135

104. Panchenko, V. M. (2009). Linhvostatystychni oznaky manipuliuvannia suspilnoiu svidomistiu v zasobakh masovoi komunikatsii. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 1 (4), 81–85.

105. Molodetska, K., Brodskiy, Yu., Fedushko, S. (2020). Model of assessment of information-psychological influence in social networking services based on information insurance. Control, Optimisation and Analytical Processing of Social Networks : Proc. of the 2nd International Workshop on COAPSN-2020, 2616, 187–198. Available at: http://ceur-ws.org/Vol-2616/paper16.pdf

106. Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A. et. al. (2018). Weaponized Health Communication: Twitter Bots and russian Trolls Amplify the Vaccine Debate. American Journal of Public Health, 108 (10), 1378–1384. doi: http://doi.org/10.2105/ajph.2018.304567

107. The official website of the World Health Organization. Available at: https://www.who.int/home

108. Molodetska, K., Tymonin, Y., Melnychuk, I. (2020). The conceptual model of information confrontation of virtual communities in social networking services. International Journal of Electrical and Computer Engineering (IJECE), 10 (1), 1043–1052. doi: http://doi.org/10.11591/ijece.v10i1.pp1043-1052

109. Leask, J., Kinnersley, P., Jackson, C., Cheater, F., Bedford, H., & Rowles, G. (2012). Communicating with parents about vaccination: a framework for health professionals. BMC Pediatrics, 12 (1). doi: http://doi.org/10.1186/1471-2431-12-154

110. Hryshchuk, R., Molodetska, K., Tymonin, Yu. (2019). Modelling of conflict interaction of virtual communities in social networking services on an example of anti-vaccination movement. Conflict Management in Global Information Networks: Proc. of the International Workshop on CMiGIN-2019, 2588, 250–264.

111. Kolesnykov, A. A. (2005). Synerhetycheskoe metody upravlenyia slozhnymy systemamy: teoryia systemnoho synteza. Edytoral URSS.

112. Hryshchuk, R., Molodetska, K. (2017). Synergetic control of social networking services actors' interactions. Recent Advances in Systems, Control and Information Technology. Springer International Publishing, 543, 34–42. doi: http://doi.org/10.1007/978-3-319-48923-0_5

113. Hryshchuk, R., Molodetska, K., Serov, Y. (2019). Method of improving the information security of virtual communities in social networking services. Proc. of the 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks, 2392, 23-41.

114. Wu, B., Cheng, T., Yip, T. L., Wang, Y. (2020). Fuzzy logic based dynamic decision-making system for intelligent navigation strategy within inland traffic separation schemes. Ocean Engineering, 197, 106909. doi: http://doi.org/10.1016/j.oceaneng.2019.106909

115. Molodetska, K., Solonnikov, V., Voitko, O., Humeniuk, I., Matsko, O., Samchyshyn, O. (2021). Counteraction to information influence in social networking services by means of fuzzy logic system. International Journal of Electrical and Computer Engineering, 11 (3), 2490–2499. doi: http://doi.org/10.11591/ijece.v11i3.pp2490-2499

116. Akgun, A., Sezer, E. A., Nefeslioglu, H. A., Gokceoglu, C., Pradhan, B. (2012). An easy-to-use MATLAB program (MamLand) for the assessment of landslide susceptibility using a Mamdani fuzzy algorithm. Computers & Geosciences, 38 (1), 23–34. doi: http://doi.org/10.1016/j.cageo.2011.04.012

117. Molodetska, K., Tymonin, Y., Markovets, O., Melnychyn, A. (2020). Phenomenological model of information operation in social networking services. Indonesian Journal of Electrical Engineering and Computer Science, 19 (2), 1078. doi: https://doi.org/10.11591/ijeecs.v19.i2.pp1078-1087

118. Synko, A., Molodetska, K. (2021). Application of Clusterization for Analysis of Virtual Community Users. Information Technologies & Applied Sciences: Proc. of the Symposium on IT&AS 2021, 2824, 9–19.

119. How the Social Networks Affect Politics in Ukraine: Conclusions of the Research (2020). Internews.Ua. Avaliable at: https://internews.ua/opportunity/social-network-research

120. Criminal complaint. Official website of the U.S. Department of Justice (DOJ). Available at: https://www.justice.gov/opa/press-release/file/1102316/download

121. Peleshchyshyn, O., Molodetska, K., Solianyk, A., Kravets, R. (2019). Modelling the complex of automation of company marketing activity in online communities. Conflict Management in Global Information Networks: Proc. of the International Workshop on CMiGIN 2019, 2588, 301–310.

122. Maddux, R. D. (2014). Arrow's theorem for incomplete relations. Journal Of Logical And Algebraic Methods In Programming, 83 (2), 235–248. doi: http://doi.org/10.1016/j.jlap.2014.02.012

123. Cato, S. (2018). Incomplete decision-making and Arrow's impossibility theorem. Mathematical Social Sciences, 94, 58–64. doi: http://doi.org/10.1016/j.mathsocsci.2017.10.002

124. Brindley, P., Cameron, R. W., Ersoy, E., Jorgensen, A., Maheswaran, R. (2019). Is more always better? Exploring field survey and social media indicators of quality of urban greenspace, in relation to health. Urban Forestry & Urban Greening, 39, 45–54. doi: http://doi.org/10.1016/j.ufug.2019.01.015

125. Public opinion poll (2020). Ilko Kucheriv Democratic Initiatives Foundation. Kyiv.

126. Karpov, A. V. (2009). Theorem on the impossibility of proportional representation. HSE Economic Journal, 4, 596–615.

127. Arrow, K. J. (1950). A Difficulty in the Concept of Social Welfare. Journal of Political Economy, 58 (4), 328–346. doi: http://doi.org/10.1086/256963

128. Vasiljev, S. (2008). Manipulability of a voting. SSRN Electronic Journal, 2008. doi: http://doi.org/10.2139/ssrn.1118627

129. Molodetska, K. (2020). Counteraction to strategic manipulations on actors' decision making in social networking services. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), 266–269. doi: http://doi.org/10.1109/atit50783.2020.9349347

130. Khromov, D. V. (2013). Models and algorithms for constructing curvilinear skeletons of spatial forms. Moscow: MV Lomonosov Moscow State University, 23.

131. Hrytsyk, V., Nazarkevych, M. (2021). Research on the Increase of Information Theory in the Era of the Ending of Silicon Electronics and New Types of Risks. CEUR Workshop Proceedingsthis, 3101, 65–82.

132. Li, J., Glover, J. D., Zhang, H., Peng, M., Tan, J., Mallick, C. B. et. al. (2022). Limb development genes underlie variation in human fingerprint patterns. Cell, 185 (1), 95–112. doi: http://doi.org/10.1016/j.cell.2021.12.008

133. Hrytsyk, V., Grondzal, A., Bilenkyj, A. (2015). Augmented reality for people with disabilities. Computer Sciences and Information Technologies, 188–191. doi: http://doi.org/10.1109/stc-csit.2015.7325462

134. Prasad, M. V. D., Krishna, N. S., Ahammad, S. H., Kumar, G. N. S. (2020). Security Systems For Identification And Detection Fingerprint Based On Cnn And Fcn. International Journal of Scientific & Technology Research 9 (2), 1668–1672.

135. Bontrager, P., Togelius, J., Memon, N. (2017). Deepmasterprint: Generating fingerprints for presentation attacks. arXiv preprint arXiv: 1705.07386.

136. Bontrager, P., Roy, A., Togelius, J., Memon, N., & Ross, A. (2018, October). Deepmasterprints: Generating masterprints for dictionary attacks via latent variable evolution. 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), 1–9. doi: http://doi.org/10.1109/btas.2018.8698539

137. Teslyuk, V. M., Beregovskyi, V. V., Pukach, A. I. (2013). Development of smart house system model based on colored Petri nets. 2013 XVIIIth International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED), 205–208.

138. Drets, G., Liljenström, H. (1998). Fingerprint Sub-Classification and Singular Point Detection. International Journal of Pattern Recognition and Artificial Intelligence, 12 (4), 407–422. doi: http://doi.org/10.1142/s0218001498000269

139. Ali, S. M., Al-Zewary, M. S. (1997). A new fast automatic technique for fingerprints recognition and identification. Journal of the Islamic Academy of Sciences, 10 (2), 55–60.

140. Cao, J., Dai, 'Q. (2009). A novel online fingerprint segmentation method based on frame-difference,'2009 International Conference on Image Analysis and Signal Processing, Taizhou, 57–60. doi: http://doi.org/10.1109/iasp.2009.5054651

141. Zhan, X., Sun, Z., Yin, Y., Chen, Y. (2005). Fingerprint image segmentation method based on MCMC & GA. In International Conference on Image Analysis and Processing. Berlin, Heidelberg: Springer, 391-398. doi: http://doi.org/10.1007/11553595_48

142. Tsmots, I., Skorokhoda, O., Rabyk, V. Structure Software Model of a Parallel-Vertical Multi-input Adder for FPGA Implementation. Computer Sciences and Information Technologies – Proceedings of the 11th International Scientific and Technical Conference CSIT 2016. Lviv, 158–160. doi: http://doi.org/10.1109/stc-csit.2016.7589894

143. Tsmots, I., Skorokhoda, O. (2010). Methods and VLSI-structures for Neural Element Implementation. Perspective Technologies and Methods in MEMS Design, MEMSTECH'2010 – Processing of the 6th International Conference. Polyana, 135.

144. Ding, Y., Zhuang, D., Wang, K. (2005). A study of hand vein recognition method. IEEE International Conference Mechatronics and Automation, 4, 2106–2110. doi: http://doi.org/10.1109/icma.2005.1626888

145. Rathgeb, C., Uhl, A. (2010). Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. In International Conference Image Analysis and Recognition. Berlin, Heidelberg: Springer, 296–305. doi: http://doi.org/10.1007/978-3-642-13775-4_30

146. Denysyuk, P., Teslyuk, V., Chorna, I. (2018). Development of mobile robot using LIDAR technology based on Arduino controller. 2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), 240–244. doi: http://doi.org/10.1109/memstech.2018.8365742

147. Kunanets, N., Vasiuta, O., Boiko, N. (2019). Advanced technologies of big data research in distributed information systems. 2019 IEEE 14th International Conference on Computer Science and Information Technologies (CSIT), 3, 71–76. doi: http://doi.org/10.1109/stc-csit.2019.8929756

148. Hore, A., Ziou, D. (2010). Image quality metrics: PSNR vs. SSIM. 2010 20th International Conference on Pattern Recognition. IEEE, 2366–2369. doi: http://doi.org/10.1109/icpr.2010.579

149. Dronyuk, I., Nazarkevych, M., Fedevych, O. (2015, October). Synthesis of Noise-Like Signal Based on Ateb-Functions. In International Conference on Distributed Computer and Communication Networks (pp. 132–140). Springer, Cham.

150. Putyatin, E. P., Panchenko, I. A. (2010). Invariance of features in problems of image processing with a pronounced texture. Radioelectronics and Informatics, 1. Available at: https://cyberleninka.ru/article/n/invariantnost-priznakov-v-zadachah-obrabotki-izobrazheniy-s-yarkovyrazhennoy-teksturoy Last accessed: 31.05.2022

151. Boyko, N., Shakhovska, N. (2018). Prospects for using cloud data warehouses in information systems. 2018 IEEE 13th International Scientific and Technical Conference on Computer Science and Information Technologies (CSIT), 2, 136–139. doi: http://doi.org/10.1109/stc-csit.2018.8526745

152. Nazarkevych, M., Voznyi, Y., Hrytsyk, V., Klyujnyk, I., Havrysh, B., Lotoshynska, N. (2021). Identification of biometric images by machine learning. 2021 IEEE 12th International Conference on Electronics and Information Technologies. ELIT 2021 – Proceedings, 95–98. doi: http://doi.org/10.1109/elit53502.2021.9501064

153. Nazarkevych, M., Kynash, Y., Oliarnyk, R., Klyujnyk, I., Nazarkevych, H. (2017). Application perfected wave tracing algorithm. 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), 1011–1014. doi: http://doi.org/10.1109/ukrcon.2017.8100403

154. Lyubchenko, V. A. (2002). Application of one-dimensional normalization in image recognition problems with projective distortions. Radio Electronics and Youth in the XXI Century. Kharkiv: KhNURE, 388–389.

155. Nazarkevych, M., Oliiarnyk, R., Nazarkevych, H., Kramarenko, O., Onyshschenko, I. (2016). The method of encryption based on Ateb-functions. 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), 129–133. doi: http://doi.org/10.1109/dsmp.2016.7583523

156. Medykovskyy, M., Lipinski, P., Troyan, O., Nazarkevych, M. (2015). Methods of protection document formed from latent element located by fractals. Computer Sciences and Information Technologies (CSIT). IEEE, 70–72. doi: http://doi.org/10.1109/stc-csit.2015.7325434

157. Süsstrunk, S., Buckley, R., Swen, S. (1999, January). Standard RGB color spaces. In Color and imaging conference (Vol. 1999, No. 1, pp. 127-134). Society for Imaging Science and Technology.

158. Dronyuk, I., Nazarkevych, M, Poplavska, Z. (2017). Gabor generalization filters based on ateb-functions for information security. InInternational Conference on Man – Machine Interactions 2017. Cham: Springer, 195–206. doi: http://doi.org/10.1007/978-3-319-67792-7_20

159. He, K., Zhang, X., Ren, S., Sun, J. (2016). Deep residual learning for image recognition. Proceedings of the IEEE conference on computer vision and pattern recognition, 770–778. doi: http://doi.org/10.1109/cvpr.2016.90

160. Wang, L., Yuan, W., Zeng, L., Xu, J., Mo, Y., Zhao, X., Peng, L. (2022). Dementia analysis from functional connectivity network with graph neural networks. Information Processing & Management, 59 (3), 102901. doi: http://doi.org/10.1016/j.ipm.2022.102901

161. Chen, Y., Sanghavi, S., Xu, H. (2012). Clustering sparse graphs. Advances in neural information processing systems, 25.

162. Arulselvan, A., Commander, C. W., Elefteriadou, L., Pardalos, P. M. (2009). Detecting critical nodes in sparse graphs. Computers & Operations Research, 36 (7), 2193–2200. doi: http://doi.org/10.1016/j.cor.2008.08.016

163. Ashraf, I., Hur, S., Park, S., Park, Y. (2020). DeepLocate: Smartphone Based Indoor Localization with a Deep Neural Network Ensemble Classifier. Sensors, 20 (1), 133. doi: http://doi.org/10.3390/s20010133

164. Chen, W., Sui, L., Xu, Z., Lang, Y. (2012). Improved Zhang-Suen thinning algorithm in binary line drawing applications. 2012 International Conference on Systems and Informatics (ICSAI2012). IEEE, 1947–1950. doi: http://doi.org/10.1109/icsai.2012.6223430

165. Saoji, S. U., Dua, N., Choudhary, A. K., Phogat, B. (2021). Air Canvas Application Using OpenCV and Numpy in Python. IRJET, 8 (8).

166. Nazarkevych, M., Oliarnyk, R., Troyan, O., Nazarkevych, H. (2016). Data protection based on encryption using Ateb-functions. 2016 XIth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT). IEEE, 30–32.

167. Nazarkevych, M., Dmytruk, S., Hrytsyk, V., Vozna, O., Kuza, A., Shevchuk, O. et. al. (2021). Evaluation of the Effectiveness of Different Image Skeletonization Methods in Biometric Security Systems. International Journal of Sensors, Wireless Communications and Control, 11 (5), 542–552. doi: http://doi.org/10.2174/2210327910666201210151809

168. Artemenko, M. V., Kalugina, N. M., Shutkin, A. N. (2016). Formation of a set of informative indicators on the basis of the Kolmogorov-Gabor approximating polynomial and the maximum gradient of functional differences. Proceedings of Southwestern State University. Series: Management, computer engineering, computer science. Medical Instrumentation, 1, 116–123.

169. Nazarkevych, M., Buriachok, V., Lotoshynska, N., Dmytryk, S. (2018). Research of Ateb-Gabor filter in biometric protection systems. 2018 IEEE 13th International Scientific and Technical Conference on Computer Science and Information Technologies (CSIT), 1, 310–313. doi: http://doi.org/10.1109/stc-csit.2018.8526607

170. Nazarkevych, M., Logoyda, M., Troyan, O., Vozniy, Y., Shpak, Z. (2019). The ateb-gabor filter for fingerprinting. Conference on Computer Science and Informatics, 247–255. doi: http://doi.org/10.1007/978-3-030-33695-0_18

171. Nazarkevych, M., Oliarnyk, R., Dmytruk, S. (2017). An images filtration using the Ateb-Gabor method. 2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), 1, 208–211. doi: http://doi.org/10.1109/stc-csit.2017.8098770

172. Nazarkevych, M., Riznyk, O., Samotyy, V., Dzelendzyak, U. (2019). Detection of regularities in the parameters of the ateb-gabor method for biometric image filtration. Eastern-European Journal of Advanced Technology, 1 (2 (97)), 57–65. doi: http://doi.org/10.15587/1729-4061.2019.154862

173. Medykovskyi, M. O., Tsmots, I. G.,Tsymbal, Y. V. (2016). Information analytical system for energy efficiency management at enterprises in the city of Lviv (Ukraine). Actual Problems in Economics, 1 (175), 379–384.

174. Dronjuk, I., Nazarkevych, M., Troyan, O. (2016). The modified amplitude-modulated screening technology for the high printing quality. InInternational Symposium on Computer and Information Sciences. Cham: Springer, 270–276. doi: http://doi.org/10.1007/978-3-319-47217-1_29

175. Nazarkevych, M., Lotoshynska, N., Brytkovskyi, V., Dmytruk, S., Dordiak, V., Pikh, I. (2019). Biometric Identification System with Ateb-Gabor Filtering. 2019 XIth International Scientific and Practical Conference on Electronics and Information Technologies (ELIT), 15–18. doi: http://doi.org/10.1109/elit.2019.8892282

176. Nazarkevych, M., Lotoshynska, N., Hrytsyk, V., Havrysh, B., Vozna, O., Palamarchuk, O. (2021). Design of biometric system and modeling of machine learning for entering the information system. International Scientific and Technical Conference on Computer Sciences and Information Technologies, 2, 225–230. doi: http://doi.org/10.1109/csit52700.2021.9648770

Edited by
Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych

MODELING OF SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURE FACILITIES

Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych,
Volodymyr Hrytsyk, Oleksandr Milov, Olha Korol, Stanislav Milevskyi, Roman Korolev,
Serhii Pohasii, Andrii Tkachov, Yevgen Melenti, Oleksandr Lavrut, Alla Havrylova,
Serhii Herasymov, Halyna Holotaistrova, Dmytro Avramenko, Roman Vozniak,
Oleksandr Voitko, Kseniia Yerhidzei, Serhii Mykus, Yurii Pribyliev, Olena Akhiiezer,
Mykhailo Shyshkin, Ivan Opirskyy, Oleh Harasymchuk, Olha Mykhaylova,
Yuriy Nakonechnyy, Marta Stakhiv, Bogdan Tomashevsky

Monograph

Technical editor I. Prudius
Desktop publishing T. Serhiienko
Cover photo Copyright © 2022 Canva