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

MODELING OF SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURE FACILITIES

Monograph

Technology
Center

2022

UDC 004.056
M78

Published in 2022
by PC TECHNOLOGY CENTER
Shatylova dacha str., 4, Kharkiv, Ukraine, 61165

Approved by the Academic Council of National Technical University «Kharkiv Polytechnic Institute», Protocol No. 5 of 01.07.2022

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

Modeling 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.

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.
Trademark Notice: product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

DOI: 10.15587/978-617-7319-57-2
ISBN 978-617-7319-57-2 (on-line)
ISBN 978-617-7319-56-5 (print)

9 786177 319572

CONTENTS

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.

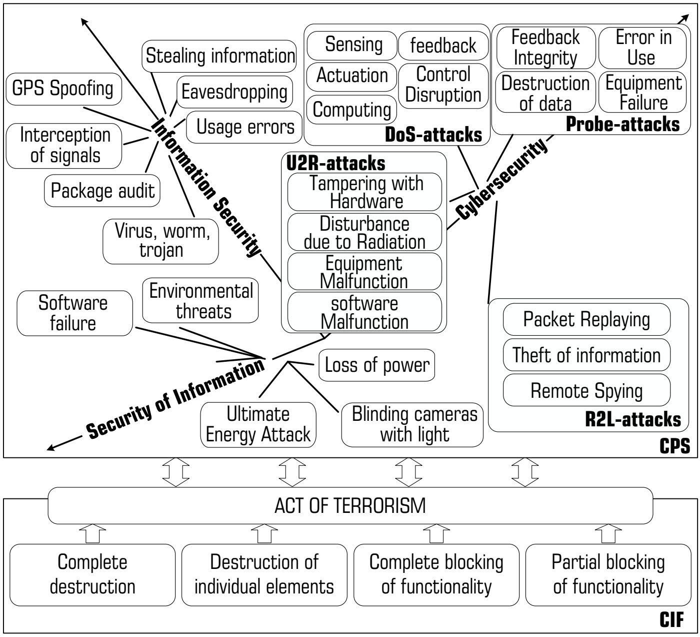


Fig. 2.1 Structural diagram of a synergistic threat model for infrastructure elements of critical infrastructure facilities

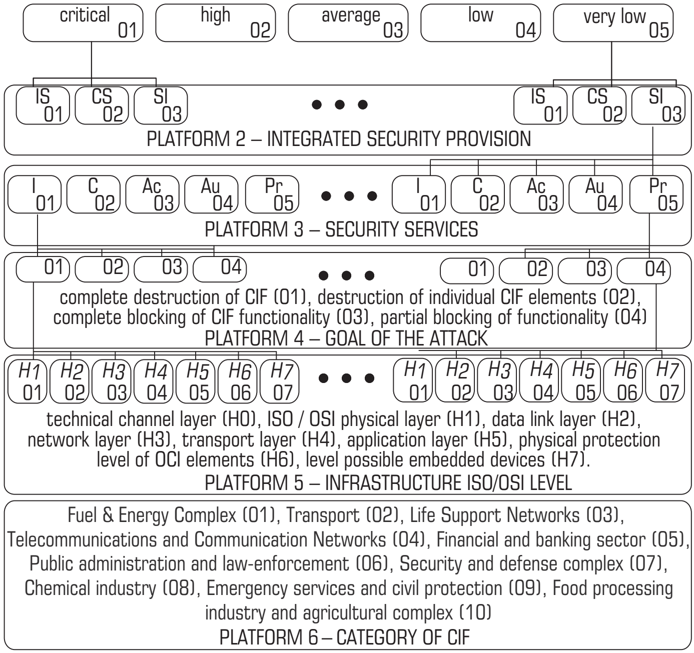

critical 01
high 02
average 03
low 04
very low 05
IS 01
CS 02
SI 03
PLATFORM 2 – INTEGRATED SECURITY PROVISION
I 01
C 02
Ac 03
Au 04
Pr 05
PLATFORM 3 – SECURITY SERVICES
01
02
03
04
complete destruction of CIF (01), destruction of individual CIF elements (02), complete blocking of CIF functionality (03), partial blocking of functionality (04)
PLATFORM 4 – GOAL OF THE ATTACK
H1 01
H2 02
H3 03
H4 04
H5 05
H6 06
H7 07
technical channel layer (H0), ISO / OSI physical layer (H1), data link layer (H2), network layer (H3), transport layer (H4), application layer (H5), physical protection level of OCI elements (H6), level possible embedded devices (H7).
PLATFORM 5 – INFRASTRUCTURE ISO/OSI LEVEL
Fuel & Energy Complex (01), Transport (02), Life Support Networks (03), Telecommunications and Communication Networks (04), Financial and banking sector (05), Public administration and law-enforcement (06), Security and defense complex (07), Chemical industry (08), Emergency services and civil protection (09), Food processing industry and agricultural complex (10)
PLATFORM 6 – CATEGORY OF CIF

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);

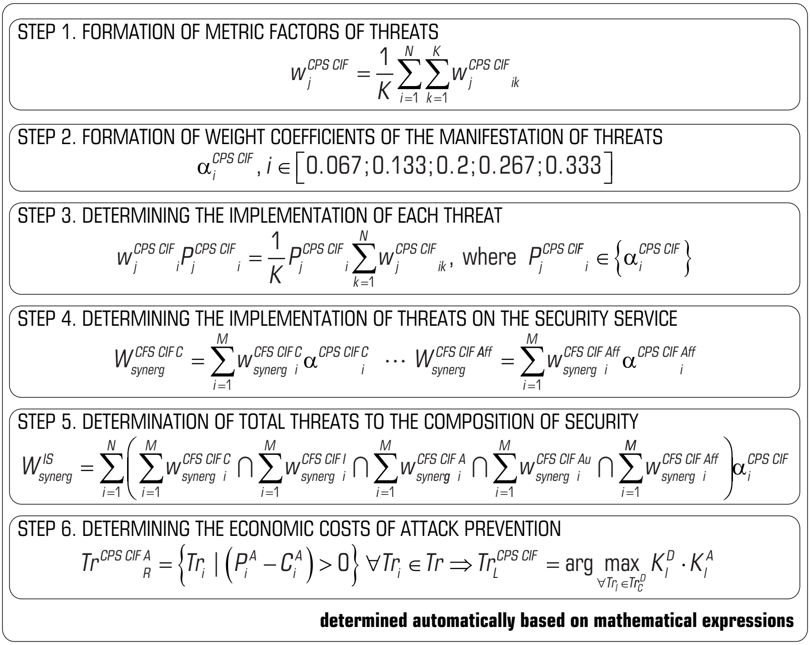
– life support networks (03);

– 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

$$W_{synerg}^{CFS\ CIF\ C} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ C}\,\alpha^{CPS\ CIF\ C}{}_i \quad \cdots \quad W_{synerg}^{CFS\ CIF\ Aff} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Aff}\,\alpha^{CPS\ CIF\ Aff}{}_i$$

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

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

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:

$$\tilde{x}_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \qquad (2.1)$$

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:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - \tilde{x}_i\right)^2. \tag{2.2}$$

The statistical probability of the obtained results 1 – α_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 σ_X^2. Then Δ defined by the expression:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \tag{2.3}$$

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

$$P_{j}^{CPS\ CIF\ A}{}_{i} \in \left\{\alpha_{i}^{CPS\ CIF\ A}{}_{i}\right\}; \tag{2.6}$$

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

where

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

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

where

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

where $w_{j}^{CFS\ CIF\ C}{}_{i}$, $w_{j}^{CFS\ CIF\ I}{}_{i}$, $w_{j}^{CFS\ CIF\ A}{}_{i}$, $w_{j}^{CFS\ CIF\ Au}{}_{i}$, $w_{j}^{CFS\ CIF\ Aff}{}_{i}$ – weight coefficients of security services: C, I, A, Au, Aff; $\alpha^{CPS\ CIF\ C}{}_{i}$, $\alpha^{CPS\ CIF\ I}{}_{i}$, $\alpha^{CPS\ CIF\ A}{}_{i}$, $\alpha^{CPS\ CIF\ Au}{}_{i}$, $\alpha^{CPS\ CIF\ Aff}{}_{i}$ – 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:

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

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

$$W_{synerg}^{CFS\ CIF\ Aff} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIF\ Aff} \alpha^{CPS\ CIF\ Aff}{}_{i}, \tag{2.7}$$

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

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:

$$P(AB) = P(A) + P(B) - P(AB). \tag{2.8}$$

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:

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

To determine the total hybrid threat:

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

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.

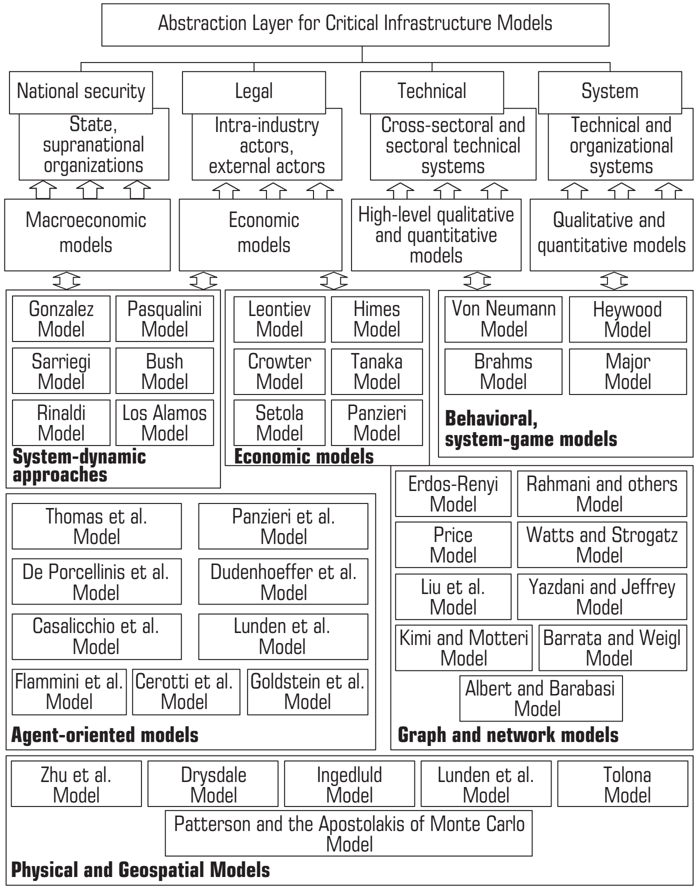


Fig. 2.4 The concept of modeling critical infrastructure objects

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:

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

where $\beta_i^{CPS\ CIF} = W_{cp}^{CPS\ CIF} \cap W_{cash}^{CPS\ CIF} \cap T$ – 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]).

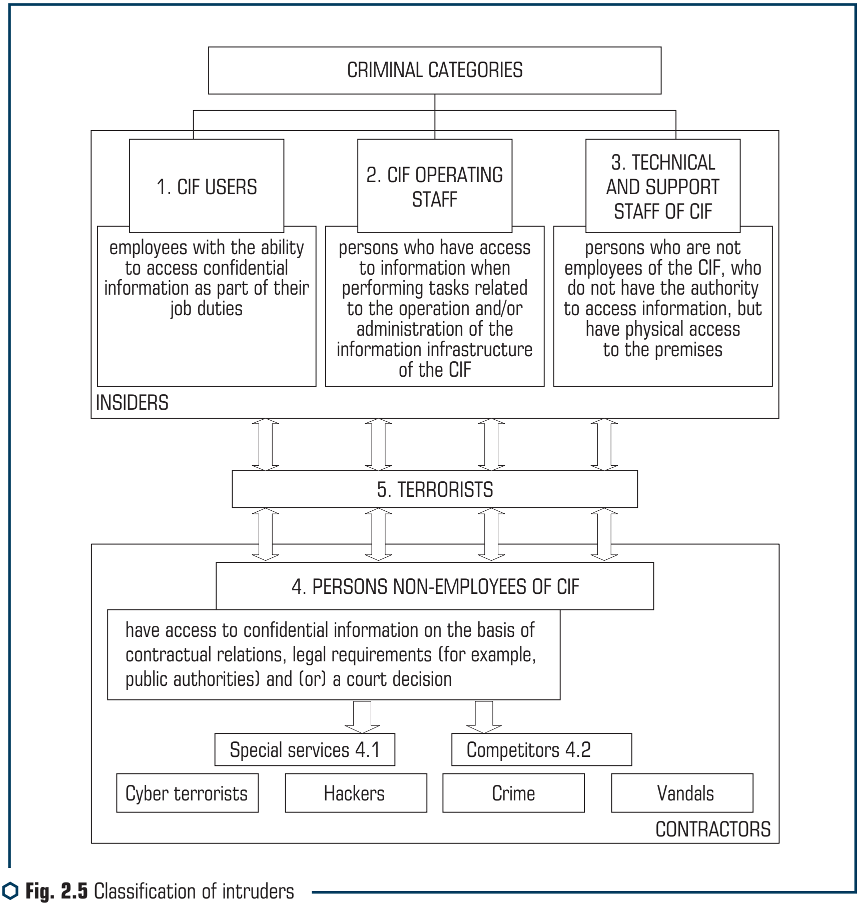

CRIMINAL CATEGORIES
1. CIF USERS
employees with the ability to access confidential information as part of their job duties
2. CIF OPERATING STAFF
persons who have access to information when performing tasks related to the operation and/or administration of the information infrastructure of the CIF
3. TECHNICAL AND SUPPORT STAFF OF CIF
persons who are not employees of the CIF, who do not have the authority to access information, but have physical access to the premises
INSIDERS
5. TERRORISTS
4. PERSONS NON-EMPLOYEES OF CIF
have access to confidential information on the basis of contractual relations, legal requirements (for example, public authorities) and (or) a court decision
Special services 4.1
Competitors 4.2
Cyber terrorists
Hackers
Crime
Vandals
CONTRACTORS

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.

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

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.

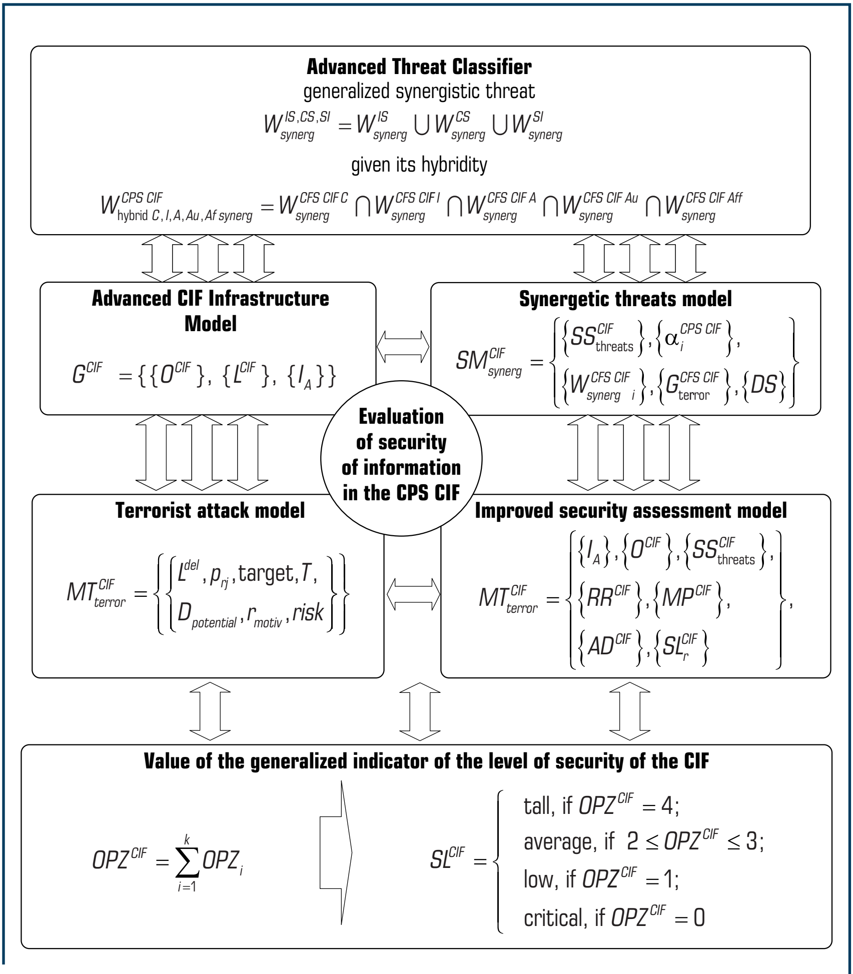

Advanced Threat Classifier
generalized synergistic threat
$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CS} \cup W_{synerg}^{SI}$
given its hybridity
$W_{\text{hybrid } C,I,A,Au,Af\ synerg}^{CPS\ CIF} = W_{synerg}^{CFS\ CIF\ C} \cap W_{synerg}^{CFS\ CIF\ I} \cap W_{synerg}^{CFS\ CIF\ A} \cap W_{synerg}^{CFS\ CIF\ Au} \cap W_{synerg}^{CFS\ CIF\ Aff}$
Advanced CIF Infrastructure Model
$G^{CIF} = \{\{O^{CIF}\},\ \{L^{CIF}\},\ \{I_A\}\}$
Synergetic threats model
$SM_{synerg}^{CIF} = \left\{ \begin{matrix} \{SS_{\text{threats}}^{CIF}\}, \{\alpha_i^{CPS\ CIF}\}, \\ \{W_{synerg\ \ i}^{CFS\ CIF}\}, \{G_{\text{terror}}^{CFS\ CIF}\}, \{DS\} \end{matrix} \right\}$
Evaluation of security of information in the CPS CIF
Terrorist attack model
$MT_{terror}^{CIF} = \left\{ \begin{Bmatrix} L^{del}, p_{rj}, \text{target}, T, \\ D_{potential}, r_{motiv}, risk \end{Bmatrix} \right\}$
Improved security assessment model
$MT_{terror}^{CIF} = \left\{ \begin{matrix} \{I_A\}, \{O^{CIF}\}, \{SS_{\text{threats}}^{CIF}\}, \\ \{RR^{CIF}\}, \{MP^{CIF}\}, \\ \{AD^{CIF}\}, \{SL_r^{CIF}\} \end{matrix} \right\},$
Value of the generalized indicator of the level of security of the CIF
$OPZ^{CIF} = \sum_{i=1}^{k} OPZ_i$
$SL^{CIF} = \begin{cases} \text{tall, if } OPZ^{CIF} = 4; \\ \text{average, if } 2 \le OPZ^{CIF} \le 3; \\ \text{low, if } OPZ^{CIF} = 1; \\ \text{critical, if } OPZ^{CIF} = 0 \end{cases}$

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: $Type=\{CI,\ PD,\ CD,\ TS,\ StR,\ PubI,\ ContI,\ PI\}$, where *CI* – confidential information, *PD* – payment documents, *CD* – credit documents, *TS* – trade secret, *StR* – statistical reports, *PubI* – public information, *ContI* – control information, *PI* – personal data. *AC, AI, AA, AAu, AAff, Acont* – security services.

Each element $O_l^{CIF}\in\{O^{CIF}\}$, described by the vector $O_l^{CIF}=\{L^{CIF}, TC^{CIF}\}$, 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:

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

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; $\{G_{\text{terror}}^{CFS\ CIF}\}$ – 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:

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

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:

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

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:

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

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:

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

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:

$$SL^{CIF} = \begin{cases} \text{tall, if } OPZ^{CIF} = 4; \\ \text{average, if } \ 2 \le OPZ^{CIF} \le 3; \\ \text{low, if } OPZ^{CIF} = 1; \\ \text{critical, if } OPZ^{CIF} = 0. \end{cases} \tag{2.28}$$

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]:

$$\begin{cases} \dfrac{dN_1}{dt} = \alpha N_1 - \beta N_1 N_2; \\ \dfrac{dN_2}{dt} = -\varphi N_2 + \gamma N_2 N_1, \end{cases} \tag{2.29}$$

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.

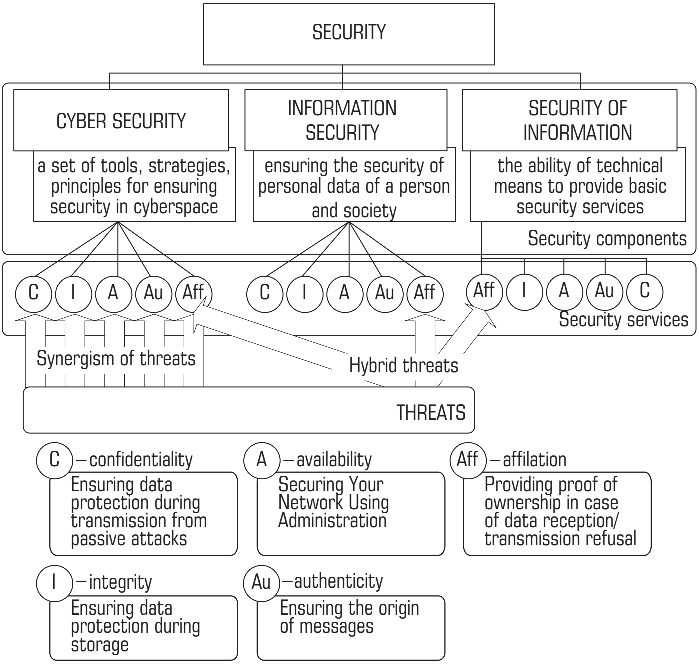

SECURITY
CYBER SECURITY
a set of tools, strategies, principles for ensuring security in cyberspace
INFORMATION SECURITY
ensuring the security of personal data of a person and society
SECURITY OF INFORMATION
the ability of technical means to provide basic security services
Security components
C
I
A
Au
Aff
Security services
Synergism of threats
Hybrid threats
THREATS
C – confidentiality
Ensuring data protection during transmission from passive attacks
A – availability
Securing Your Network Using Administration
Aff – affilation
Providing proof of ownership in case of data reception/ transmission refusal
I – integrity
Ensuring data protection during storage
Au – authenticity
Ensuring the origin of messages

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:

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

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:

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

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:

$$Tr_R^A = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \forall Tr_i \in Tr, \tag{2.32}$$

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:

$$Tr_C^D = \left\{ Tr_j \mid \left(P_i^D - C_i^D \right) > 0 \right\} \forall Tr_j \in Tr, \tag{2.33}$$

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:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M} \left(P_i^A - C_i^A \right)}, \forall Tr_i \in Tr_R^A, M = \left| Tr_R^A \right|, \tag{2.34}$$

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:

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

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 $\left|\{W_{hybrid\ C,I,A,Au,Af}\}\right|_{synerg}$ – the power of the set of hybrid threats (i.e., their number), and $\{W_{hybrid\ C,I,A,Au,Af}\}_{synerg}$ – 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}
	$f(N) = r + \lVert A \rVert \times N$	T^{CPS}	$\lVert A \rVert$		
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:

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

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: $\Delta t_{[i-q]}(t)=K/I(t)$, 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:

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

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:

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

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:

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

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:

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

where the coefficients ε, ζ>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.

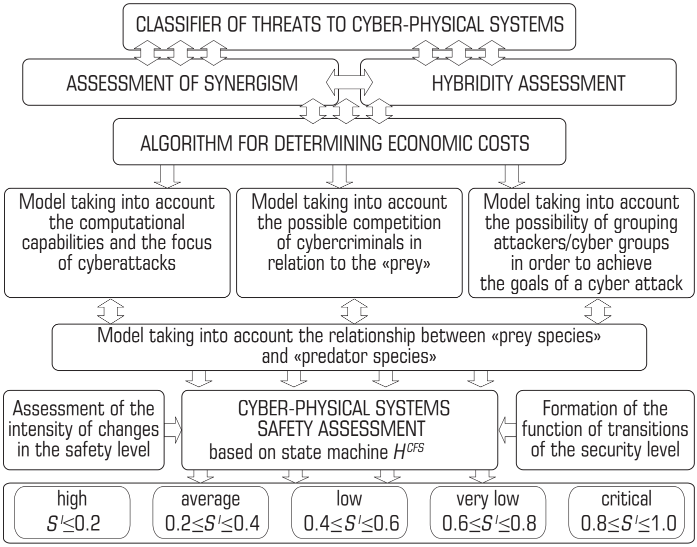

CLASSIFIER OF THREATS TO CYBER-PHYSICAL SYSTEMS
ASSESSMENT OF SYNERGISM
HYBRIDITY ASSESSMENT
ALGORITHM FOR DETERMINING ECONOMIC COSTS
Model taking into account the computational capabilities and the focus of cyberattacks
Model taking into account the possible competition of cybercriminals in relation to the «prey»
Model taking into account the possibility of grouping attackers/cyber groups in order to achieve the goals of a cyber attack
Model taking into account the relationship between «prey species» and «predator species»
Assessment of the intensity of changes in the safety level
CYBER-PHYSICAL SYSTEMS SAFETY ASSESSMENT based on state machine H^{CFS}
Formation of the function of transitions of the security level
high $S^l \leq 0.2$
average $0.2 \leq S^l \leq 0.4$
low $0.4 \leq S^l \leq 0.6$
very low $0.6 \leq S^l \leq 0.8$
critical $0.8 \leq S^l \leq 1.0$

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 cyber-physical 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.

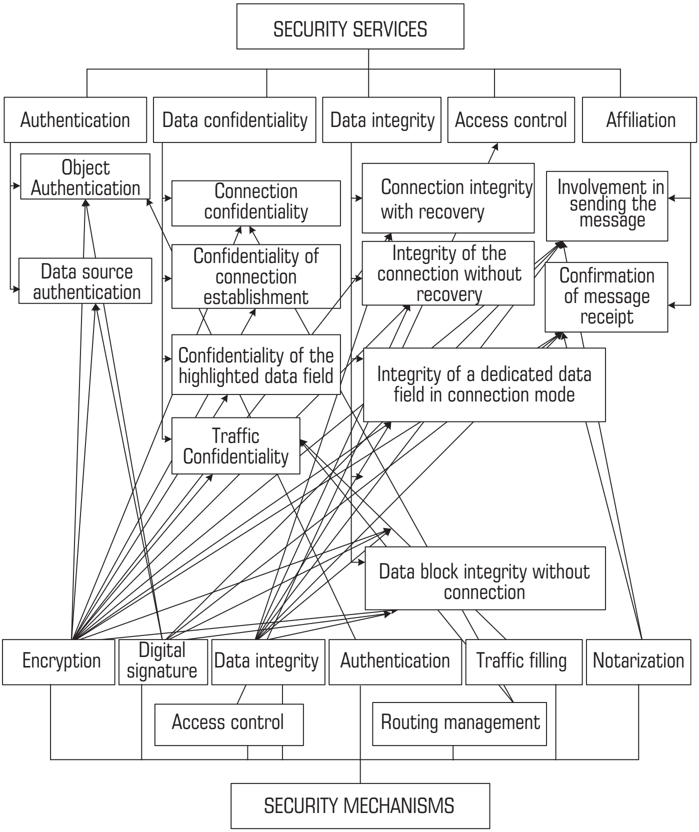

SECURITY SERVICES
Authentication
Data confidentiality
Data integrity
Access control
Affiliation
Object Authentication
Connection confidentiality
Connection integrity with recovery
Involvement in sending the message
Data source authentication
Confidentiality of connection establishment
Integrity of the connection without recovery
Confirmation of message receipt
Confidentiality of the highlighted data field
Integrity of a dedicated data field in connection mode
Traffic Confidentiality
Data block integrity without connection
Encryption
Digital signature
Data integrity
Authentication
Traffic filling
Notarization
Access control
Routing management
SECURITY MECHANISMS

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:

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

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:

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

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:

$$\alpha = \frac{\left|\{Tr_l\}\right|}{Q} = \frac{29}{194} = 0.15. \tag{2.51}$$

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

$\left|W_{\text{hybrid}\, C,I,A,Au,Af\ synerg}\right| = 0.03$, 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 cybercriminals every day. The coefficient β of the impact of modern threats on protective equipment, presented earlier as:

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

largely depends on expert assessments. Based on the opinion of experts, let's get the value of the coefficient β=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					
$w_j^{CPS\ CIF}$	$w_{CPS\,i}^{\ C}$	$w_{CPS\,i}^{\ Au}$	$w_{CPS\,i}^{\ A}$	$w_{CPS\,i}^{\ I}$	$w_{CPS\,i}^{\ Aff}$
	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 $M = \left|\{Tr_l\}\right|$. 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 $\mu^j = \left|\{C_r^j, S_c^j, O_E^j\}\right|$, 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.

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

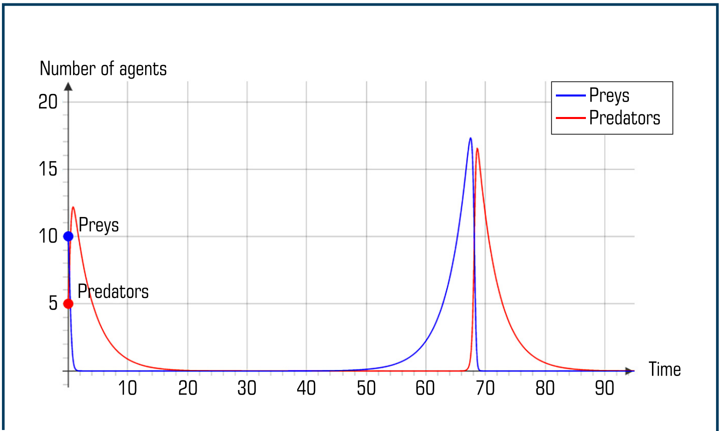
$$\tilde{N}_2 = N_2 \times \left|W_{hybrid\ C,I,A,Au,Af\ synerg}\right| = 5 \times 9 = 45.$$

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).

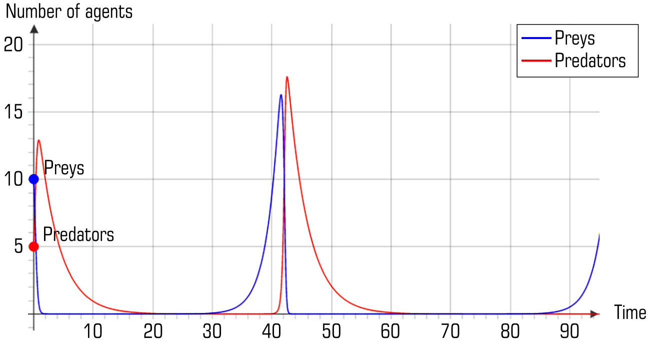


Fig. 2.11 Reduction of the oscillation period in the «predator-prey» system, $\alpha=0.49$, $\beta=0.32$, $\gamma=0.29$, $\varphi=0.29$

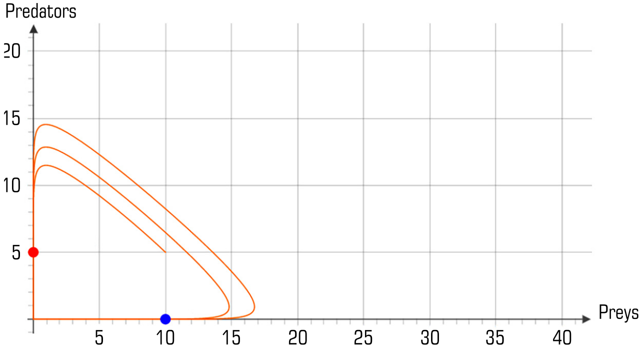


Fig. 2.12 Phase portrait of the CFR dynamics (basic version), with $\alpha=0.28$, $\beta=0.33$, $\gamma=0.29$, $\varphi=0.28$

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**.

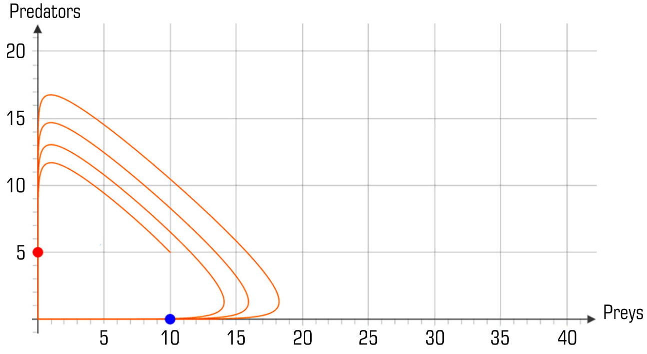


Fig. 2.13 Phase portrait with a change in the birth rate of preys, with $\alpha=0.39$, $\beta=0.32$, $\gamma=0.29$, $\varphi=0.27$

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**).

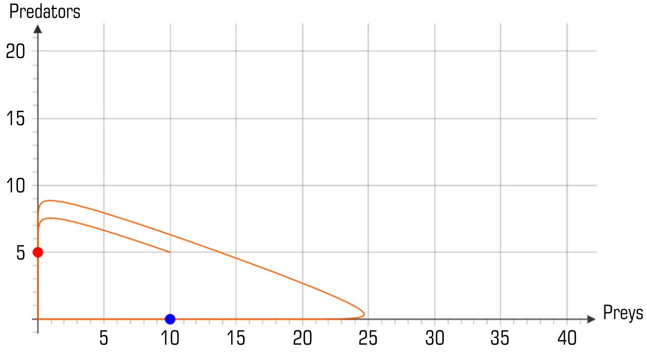
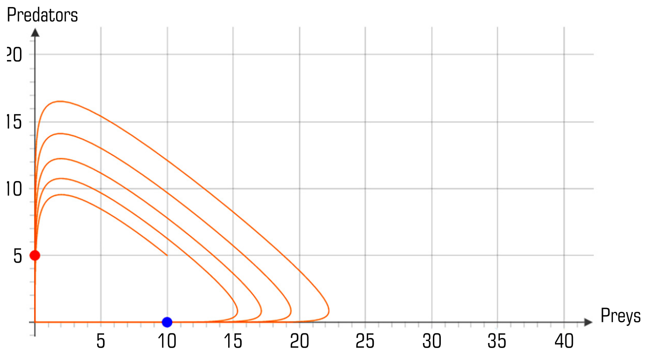


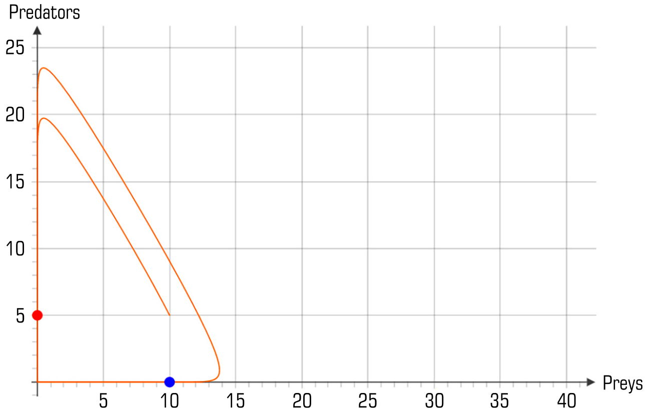
Fig. 2.14 Phase portrait of the system with an increase in the influence of predators on prey (more aggressive conduct of cyberattacks), with $\alpha=0.25$, $\beta=0.76$, $\gamma=0.29$, $\varphi=0.27$

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-GRUNDSHULTZ	+	–	–	–	–	–	–	+	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 $Q_{synerg}=Q\times\beta=194\times0.32=62.08$). 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.

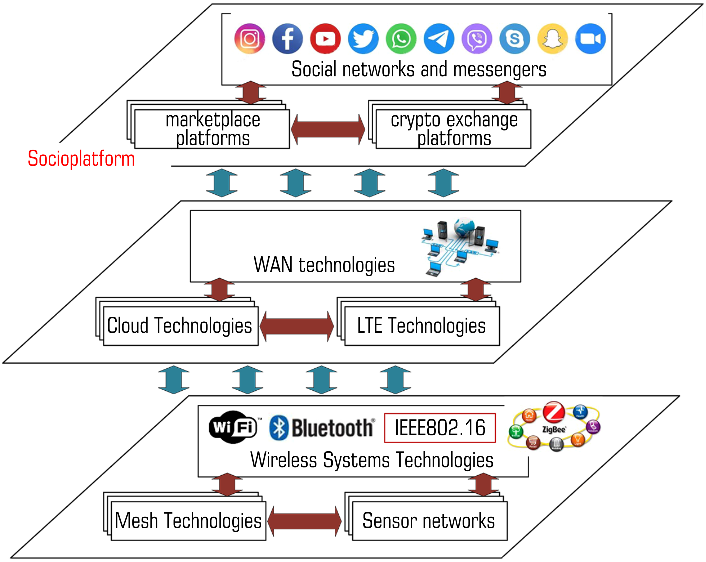


Fig. 2.17 Structural-logical scheme of socio-cyber-physical systems

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.

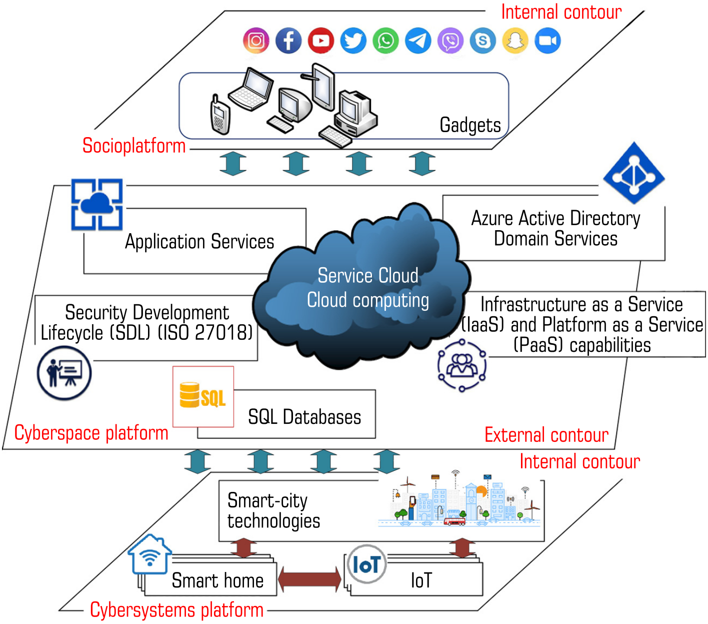


Fig. 2.18 Structural-physical scheme of socio-cyber-physical systems

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.

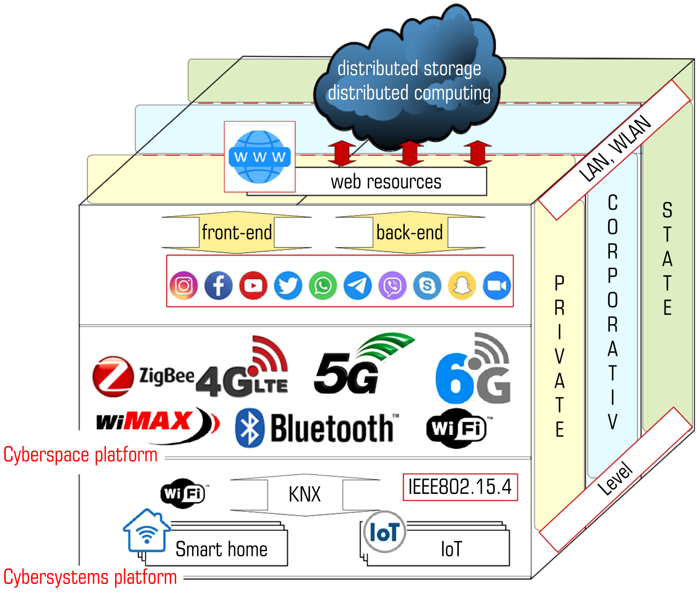


Fig. 2.19 Structural scheme of the Concept of multi-loop security of socio-cyber-physical systems

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.

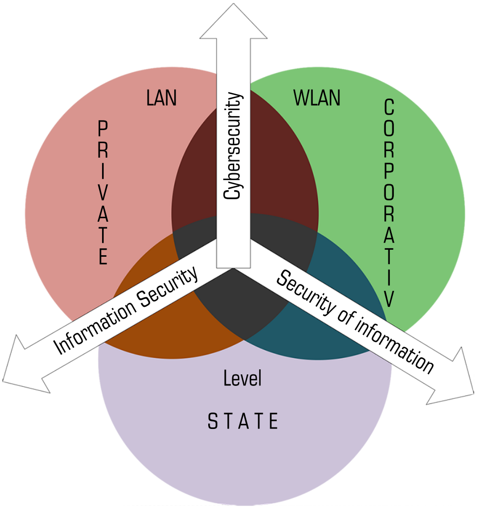


Fig. 2.20 Structural and logical scheme of threats to socio-cyber-physical systems, taking into account the form of power

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:

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

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

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

$W^{SS\ ISL}_{synerg_{1platform}}{}^{Au}$ – synergy of threats to the authenticity service; $W^{SS\ ISL}_{synerg_{1platform}}{}^{Inv}$ – 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:

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

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

where $W^{CS\ ISL}_{synerg_{2platform}}{}^{C}$ – synergy of threats to the confidentiality service; $W^{CS\ ISL}_{synerg_{2platform}}{}^{I}$ – synergy of threats to the integrity service; $W^{CS\ ISL}_{synerg_{2platform}}{}^{A}$ – synergy of threats to the availability service; $W^{CS\ ISL}_{synerg_{2platform}}{}^{Au}$ – synergy of threats to the authenticity service; $W^{CS\ ISL}_{synerg_{2platform}}{}^{Inv}$ – 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:

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

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

where $W^{CPS\ ISL}_{synerg_{3platform}}{}^{C}$ – synergy of threats to the confidentiality service; $W^{CPS\ ISL}_{synerg_{3platform}}{}^{I}$ – synergy of threats to the integrity service; $W^{CS\ ISL}_{synerg_{3platform}}{}^{A}$ – synergy of threats to the availability service; $W^{CS\ ISL}_{synerg_{3platform}}{}^{Au}$ – synergy of threats to the authenticity service; $W^{CS\ ISL}_{synerg_{2platform}}{}^{Inv}$ – 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:

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

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**):

$$W^{CPSS}_{ISL_{general}} = W^{CPSS}_{ISL_{private.}} \bigcup W^{CPSS}_{ISL_{state}} \bigcup W^{CPSS}_{ISL_{corporativ}}, \qquad (2.56)$$

where $W^{CPSS}_{ISL_{private.}}$ – overall assessment of internal loop threats to the personal property system; $W^{CPSS}_{ISL_{state}}$ – overall assessment of threats of the internal loop for the state property system; $W^{CPSS}_{ISL_{corporativ}}$ – 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:

$$W^{SS\ ESL}_{\mathrm{hybrid}\ C,I,A,Au,Af\ synerg\ _{1\mathrm{platform}}} =$$

$$= W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{C} \cap W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{I} \cap W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{A} \cap W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{Au} \cap W^{SCPS\ ESL}_{synerg_{1\mathrm{platform}\ \partial}}{}^{Inv}, \tag{2.57}$$

where $W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{C}$ – synergy of threats to the confidentiality service; $W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{I}$ – synergy of threats to the integrity service; $W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{A}$ – synergy of threats to the availability service; $W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{Au}$ – synergy of threats to the authenticity service; $W^{SS\ ESL}_{synerg_{1\mathrm{platform}}}{}^{Inv}$ – 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:

$$W^{CS\ ESL}_{\mathrm{hybrid}\ C,I,A,Au,Af\ synerg_{2\mathrm{platform}}} =$$

$$= W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{C} \cap W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{I} \cap W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{A} \cap W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{Au} \cap W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{Inv}, \tag{2.58}$$

where $W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{C}$ – synergy of threats to the confidentiality service; $W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{I}$ – synergy of threats to the integrity service; $W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{A}$ – synergy of threats to the availability service; $W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{Au}$ – synergy of threats to the authenticity service; $W^{CS\ ESL}_{synerg_{2\mathrm{platform}}}{}^{Inv}$ – 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:

$$W^{CPS\ ESL}_{\mathrm{hybrid}\ C,I,A,Au,Af\ synerg_{3\mathrm{platform}}} =$$

$$= W^{CPS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{C} \cap W^{CPS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{I} \cap W^{CPS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{A} \cap W^{CPS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{Au} \cap W^{CPS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{Inv}, \tag{2.59}$$

where $W^{CPS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{C}$ – synergy of threats to the confidentiality service; $W^{CPS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{I}$ – synergy of threats to the integrity service; $W^{CS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{A}$ – synergy of threats to the availability service; $W^{CS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{Au}$ – synergy of threats to the authenticity service; $W^{CS\ ESL}_{synerg_{3\mathrm{platform}}}{}^{Inv}$ – 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:

$$W^{CPSS}_{ESL} = W^{SS\ ESL}_{\mathrm{hybrid}\ C,I,A,Au,Af\ synerg_{1\mathrm{platform}}} \cup W^{CS\ ESL}_{\mathrm{hybrid}\ C,I,A,Au,Af\ synerg_{2\mathrm{platform}}} \cup W^{CPS\ ESL}_{\mathrm{hybrid}\ C,I,A,Au,Af\ synerg_{3\mathrm{platform}}}. \tag{2.60}$$

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**):

$$W_{ESL_{\text{general}}}^{CPSS} = W_{ESL_{\text{private.}}}^{CPSS} \cup W_{ESL_{\text{state}}}^{CPSS} \cup W_{ESL_{\text{corporativ}}}^{CPSS}, \tag{2.61}$$

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

$$W_{\text{final}}^{CPSS} = W_{ISL_{\text{general}}}^{CPSS} \cup W_{ESL_{\text{general}}}^{CPSS}. \tag{2.62}$$

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*$_i$, *PubI*$_i$, *ContI*$_i$, *PI*$_i$}, where *CI*$_i$ – confidential information, *PD*$_i$ – payment documents, *CD*$_i$ – loan documents, *TS*$_i$ – commercial secret, *StR*$_i$ – statistical reports, *PubI*$_i$ – public information, *ContI*$_i$ – 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:

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

– for multiplicative convolution:

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

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**.

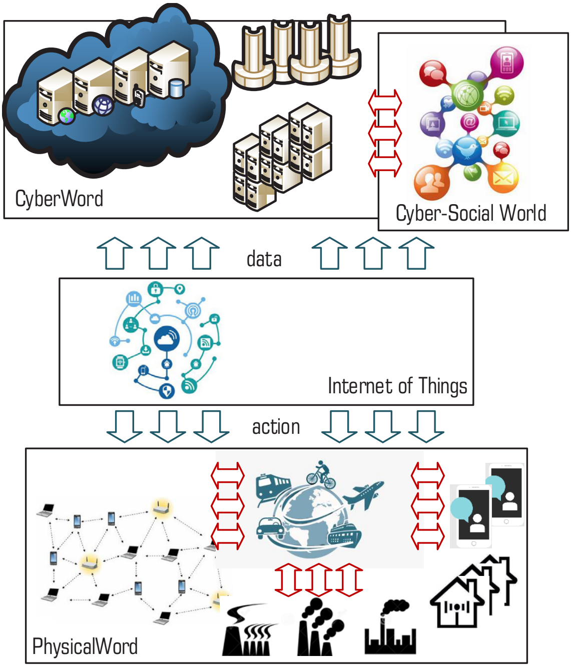


Fig. 2.21 Block diagram of the interaction of CPSS elements

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**.

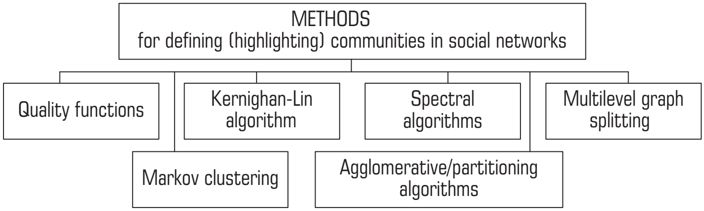

METHODS
for defining (highlighting) communities in social networks
Quality functions
Kernighan-Lin algorithm
Spectral algorithms
Multilevel graph splitting
Markov clustering
Agglomerative/partitioning algorithms

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:

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

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**.

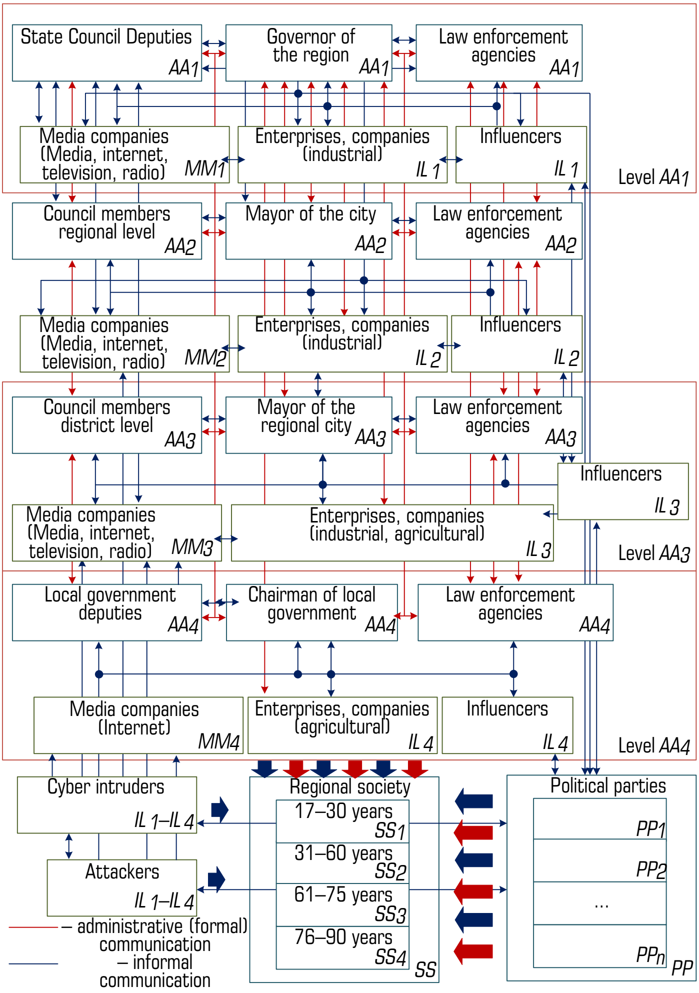

State Council Deputies AA1
Governor of the region AA1
Law enforcement agencies AA1
Media companies (Media, internet, television, radio) MM1
Enterprises, companies (industrial) IL 1
Influencers IL 1
Level AA1
Council members regional level AA2
Mayor of the city AA2
Law enforcement agencies AA2
Media companies (Media, internet, television, radio) MM2
Enterprises, companies (industrial) IL 2
Influencers IL 2
Council members district level AA3
Mayor of the regional city AA3
Law enforcement agencies AA3
Influencers IL 3
Media companies (Media, internet, television, radio) MM3
Enterprises, companies (industrial, agricultural) IL 3
Level AA3
Local government deputies AA4
Chairman of local government AA4
Law enforcement agencies AA4
Media companies (Internet) MM4
Enterprises, companies (agricultural) IL 4
Influencers IL 4
Level AA4
Cyber intruders IL 1–IL 4
Attackers IL 1–IL 4
Regional society
17–30 years SS1
31–60 years SS2
61–75 years SS3
76–90 years SS4
SS
Political parties
PP1
PP2
...
PPn
PP
– administrative (formal) communication
– informal communication

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:

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

– for informal leaders:

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

– for the media:

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

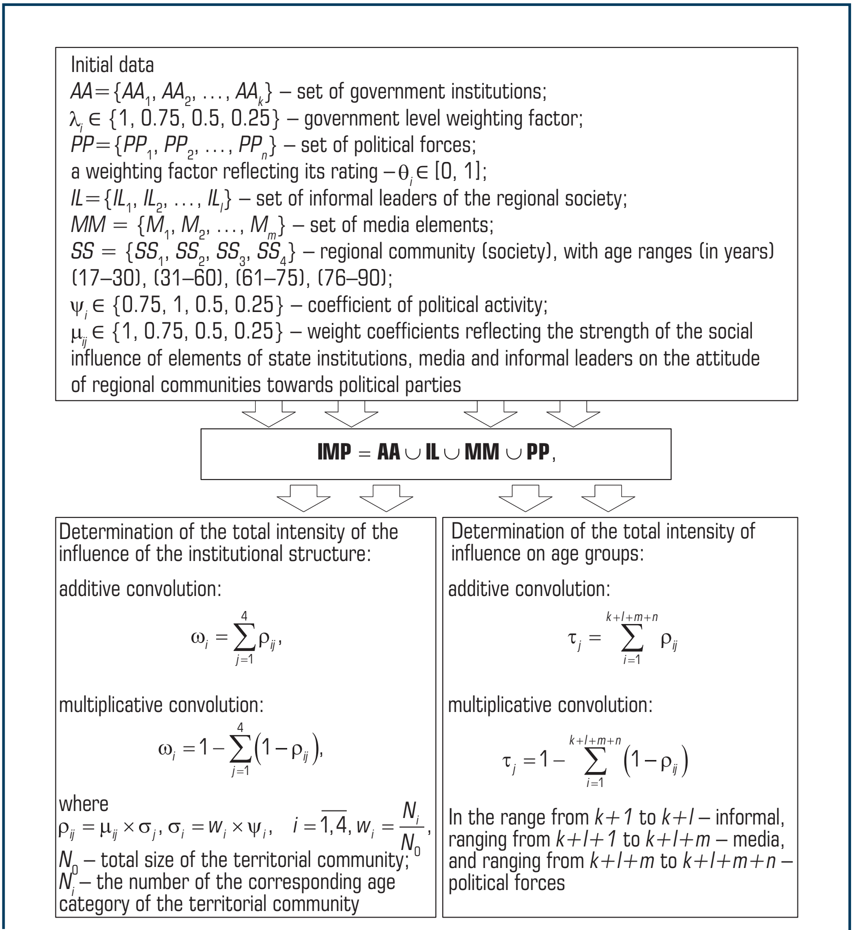
– for political parties:

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

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 $-\theta_i \in [0, 1]$;
$IL=\{IL_1, IL_2, \ldots, IL_l\}$ – 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
$\rho_{ij} = \mu_{ij} \times \sigma_j,\ \sigma_i = w_i \times \psi_i,\quad i = \overline{1,4},\ w_i = \dfrac{N_i}{N_0},$
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:

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

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:

$$\rho_{ij}=\mu_{ij}\times\sigma_j. \tag{2.79}$$

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

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

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**.

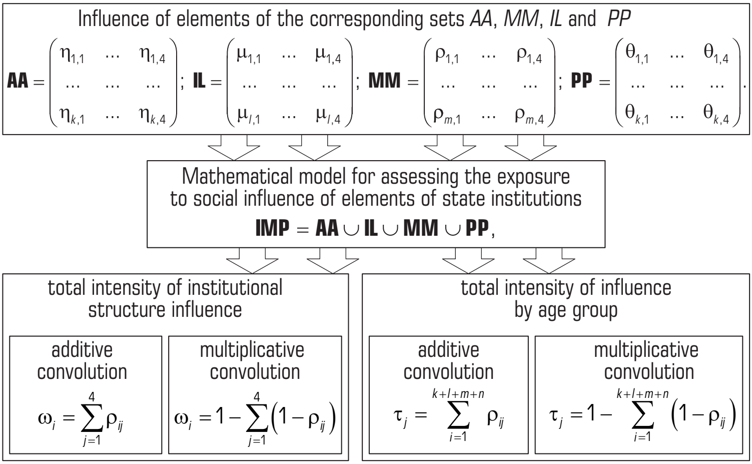

Influence of elements of the corresponding sets *AA*, *MM*, *IL* and *PP*
$\mathbf{AA} = \begin{pmatrix} \eta_{1,1} & \dots & \eta_{1,4} \\ \dots & \dots & \dots \\ \eta_{k,1} & \dots & \eta_{k,4} \end{pmatrix}; \mathbf{IL} = \begin{pmatrix} \mu_{1,1} & \dots & \mu_{1,4} \\ \dots & \dots & \dots \\ \mu_{l,1} & \dots & \mu_{l,4} \end{pmatrix}; \mathbf{MM} = \begin{pmatrix} \rho_{1,1} & \dots & \rho_{1,4} \\ \dots & \dots & \dots \\ \rho_{m,1} & \dots & \rho_{m,4} \end{pmatrix}; \mathbf{PP} = \begin{pmatrix} \theta_{1,1} & \dots & \theta_{1,4} \\ \dots & \dots & \dots \\ \theta_{k,1} & \dots & \theta_{k,4} \end{pmatrix}.$
Mathematical model for assessing the exposure to social influence of elements of state institutions
$\mathbf{IMP} = \mathbf{AA} \cup \mathbf{IL} \cup \mathbf{MM} \cup \mathbf{PP},$
total intensity of institutional structure influence
additive convolution
$\omega_i = \sum_{j=1}^{4} \rho_{ij}$
multiplicative convolution
$\omega_i = 1 - \sum_{j=1}^{4} \left(1 - \rho_{ij}\right)$
total intensity of influence by age group
additive convolution
$\tau_j = \sum_{i=1}^{k+l+m+n} \rho_{ij}$
multiplicative convolution
$\tau_j = 1 - \sum_{i=1}^{k+l+m+n} \left(1 - \rho_{ij}\right)$

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.

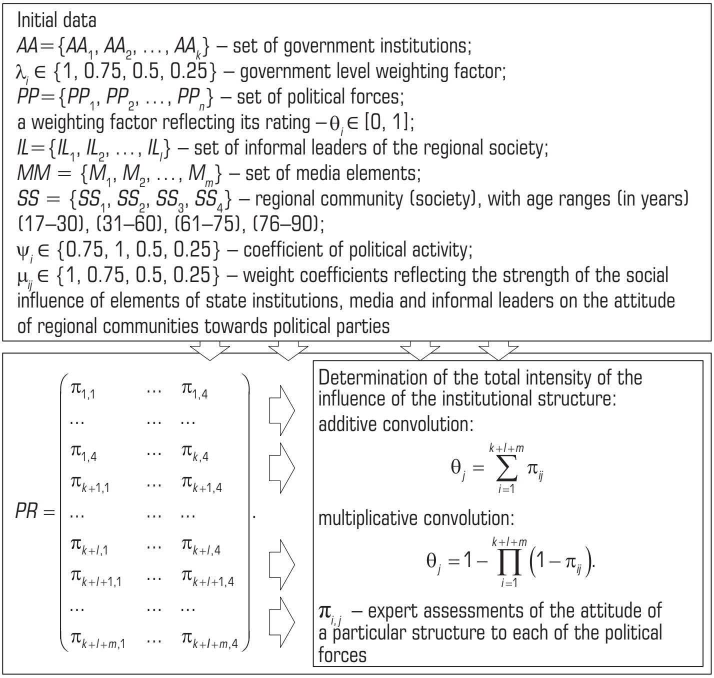
Development of a method for assessing and predicting the rating of political forces based on the mechanism of social influence

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:

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

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.



Initial data

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

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

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

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

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

$MM = \{M_1, M_2, \dots, M_m\}$ – 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

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

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

additive convolution:

$$\theta_j = \sum_{i=1}^{k+l+m} \pi_{ij}$$

multiplicative convolution:

$$\theta_j = 1 - \prod_{i=1}^{k+l+m} \left(1 - \pi_{ij}\right).$$

$\pi_{i,j}$ – expert assessments of the attitude of a particular structure to each of the political 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 – $\theta_j = \sum_{i=1}^{k+l+m} \pi_{ij}$;

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

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

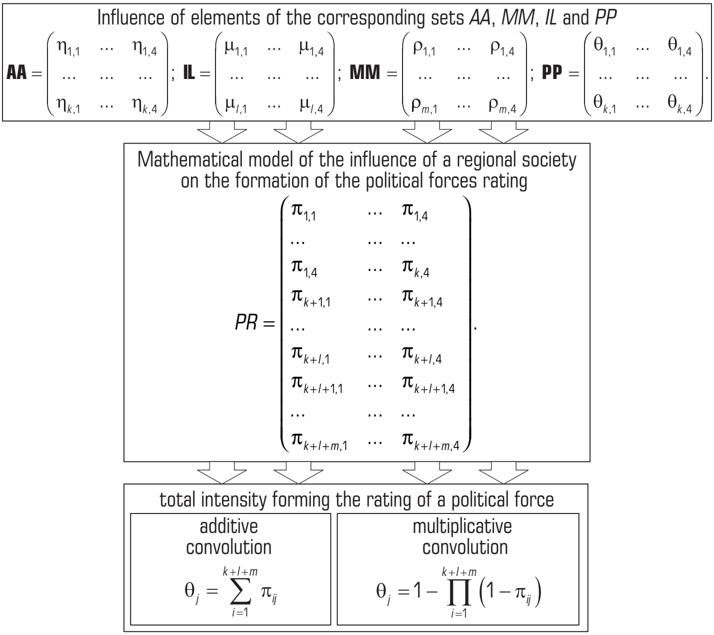

Influence of elements of the corresponding sets *AA*, *MM*, *IL* and *PP*
$\mathbf{AA} = \begin{pmatrix} \eta_{1,1} & \dots & \eta_{1,4} \\ \dots & \dots & \dots \\ \eta_{k,1} & \dots & \eta_{k,4} \end{pmatrix}$; $\mathbf{IL} = \begin{pmatrix} \mu_{1,1} & \dots & \mu_{1,4} \\ \dots & \dots & \dots \\ \mu_{l,1} & \dots & \mu_{l,4} \end{pmatrix}$; $\mathbf{MM} = \begin{pmatrix} \rho_{1,1} & \dots & \rho_{1,4} \\ \dots & \dots & \dots \\ \rho_{m,1} & \dots & \rho_{m,4} \end{pmatrix}$; $\mathbf{PP} = \begin{pmatrix} \theta_{1,1} & \dots & \theta_{1,4} \\ \dots & \dots & \dots \\ \theta_{k,1} & \dots & \theta_{k,4} \end{pmatrix}$.
Mathematical model of the influence of a regional society on the formation of the political forces rating
$PR = \begin{pmatrix} \pi_{1,1} & \dots & \pi_{1,4} \\ \dots & \dots & \dots \\ \pi_{1,4} & \dots & \pi_{k,4} \\ \pi_{k+1,1} & \dots & \pi_{k+1,4} \\ \dots & \dots & \dots \\ \pi_{k+l,1} & \dots & \pi_{k+l,4} \\ \pi_{k+l+1,1} & \dots & \pi_{k+l+1,4} \\ \dots & \dots & \dots \\ \pi_{k+l+m,1} & \dots & \pi_{k+l+m,4} \end{pmatrix}$.
total intensity forming the rating of a political force
additive convolution
$\theta_j = \sum_{i=1}^{k+l+m} \pi_{ij}$
multiplicative convolution
$\theta_j = 1 - \prod_{i=1}^{k+l+m} \left(1 - \pi_{ij}\right)$

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.