A. A. Shyian, L. O. Nikiforova

ENSURING INFORMATION SECURITY AND CYBERSECURITY IN THE MODERN INFORMATION SPACE: MODELS AND METHODS

Ministry of Education and Science of Ukraine
Vinnytsia National Technical University

A. A. Shyian, L. O. Nikiforova

ENSURING INFORMATION SECURITY AND CYBERSECURITY IN THE MODERN INFORMATION SPACE: MODELS AND METHODS

Monograph

Vinnytsia
VNTU
2024

UDC 331.101.3
S56

Recommended for publication by the Academic Council of Vinnytsia National Technical University of the Ministry of Education and Science of Ukraine (Minutes № 6 of 27.01.2022)

Reviewers:

S. D. Shtovba, Doctor of Technical Sciences, Professor

V. V. Karpinets, Candidate of Technical Sciences, Associate Professor

Shyian, A. A.

S56 Ensuring information security and cybersecurity in the modern information space: models and methods : Monograph [Electronic resource] / A. A. Shyian, L. O. Nikiforova. Vinnytsia : VNTU, 2024, (PDF, 135 p.)

ISBN 978-617-8163-02-0 (PDF)

The monograph addresses the need to counteract cybersecurity threats; analysis of modern models and methods of information security management; development of an effective method for detecting threat agents in cybersecurity tasks and a method for building an information space of information security subjects, etc. The monograph is intended for scientists, graduate students and masters and a wide range of cybersecurity specialists.

UDC 331.101.3

ISBN 978-617-8163-02-0 (PDF)

CONTENT

Introduction

The reasons for the violation of information security and the vast majority of incidents are people. It is people's behavior, which, due to subjective reasons, leads to a violation of norms and rules developed to ensure information security.

Today, there are a large number of mathematical models, the use of which can reduce the level of risk and increase the protection of information. However, the realities of applying these models, norms and rules by both individuals and social groups often indicate their violation. This is especially evident in the tasks of cybersecurity, which are aimed at ensuring the protection of information security subjects from negative information influence, from information attacks.

The scientific study of the reaction of both an individual and social groups to a negative information impact, to a targeted information attack still does not allow to make an effective forecast of the behavior of subjects and to develop effective measures to counteract such attacks. Despite some results obtained along this path, the practical implementation of a number of recommendations encounters serious resistance from the subjects of information security themselves. A significant part of practical measures to counteract information attacks is based on technologies to restrict subjects from accessing information that is considered harmful to them. This is what causes significant resistance from both individuals and numerous social groups. This is caused, for example, by objective reasons, when the restriction of access harms the performance of functional duties by employees. This is also caused by social reasons, when the subjects of information security react extremely negatively to the restriction of their access to information. Because the current development of society corresponds to the level of the information society, where the very restriction of access to information can be considered as an information attack on the main mechanisms of existence of such a society.

On the way to further development of society, the contradiction between the need to provide access to the widest possible range of information and the need to protect both individuals and society as a whole from negative information impact will only grow. For example, with the growth of the amount of information accumulated by society, which is necessary for its functioning, the number of people who are able to rationally operate only with certain fragments of this general information is rapidly growing. They are forced to perceive other fragments of the general information of society uncritically. It is this feature of the functioning of society that is often the target of an information attack today.

This situation is typical for any society, both developed and developing. This is clearly seen in the example of the emergence of a spontaneous movement of "anti-vaxxers" against the backdrop of the COVID pandemic. It is quite significant that even scientists are involved in this movement.

Thus, the development of models and methods that have on me to ensure information security and cybersecurity in the modern information space is relevant in scientific and important in practical application problem. Approaches to resolving the contradiction between the need to provide people with free access to any information and the need to protect people from harmful information are gradually becoming the main focus of research in the field of information and cybersecurity.

CHAPTER 1. ANALYSIS OF MODELS AND METHODS OF PROTECTION OF SUBJECTS OF INFORMATION SECURITY AND CYBERSECURITY

1.1 The need to counter threats to information security and cybersecurity

Cybersecurity is part of the information security of any organization [01]. Information security is the security of information, usually of an organization or company, including in IT systems.

The weakest link in any security system is always the same – people. No matter how comprehensive, effective or expensive your security tools are, all this can fail if one careless user makes one simple mistake [05].

The objects of information security can be: consciousness, psyche of people; information systems of various scales and for various purposes. The social objects of information security usually include the individual, collective, society, state, world community [02]. In this work, as agents or subjects of information security in the information space and cyberspace will act exactly social and object and information security, namely the person, social group and society.

The Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine" [03] gives the following definition: "Cybersecurity is the protection of vital interests of man and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace".

Information security of the state (society) is characterized by the degree of protection of the state (society) and stability of the main spheres of life (economy, science, technosphere, management, military affairs, etc.) against dangerous (destabilizing, destructive, affecting state interests, etc.) information influences, both for the introduction and extraction of information. Information security of the state is determined by the ability to neutralize such influences.

The National Security Strategy of Ukraine, enacted by the Decree of the President of Ukraine 392/2020 of September 14, 20, 20 [04] in para.Fig. 1.1 and 1.6 define, among the priorities of Ukraine's national interests and ensuring national security , the goals and main directions of state policy in the sphere of national security are as follows**:**

– "A person, their life and health, honor and dignity, inviolability and security are the highest social value in Ukraine".

– "Strengthening the capabilities of the national cybersecurity system to effectively counter cyber threats in the modern security environment".

In turn, the information security of the individual is the protection of the human psyche and consciousness from dangerous information influences: manipulation of consciousness, misinformation, incitement to suicide, insults, etc. [02].

Thus, ensuring the information and psychological security of a person and a social group is defined by the Strategy as one of the main factors in countering external threats, and the creation of modern information and psychological security management systems is defined in the National Security Strategy of Ukraine as one of the main tasks.

Also, the approved Strategy identifies current and projected threats to national security and national interests of Ukraine, taking into account foreign policy and domestic conditions. In particular, in paragraphs 2.9, 2.14 and 2.17 respectively [04]:

– "The role of information technology in all spheres of public life is growing rapidly."

– "The competition between the United States of America and the People's Republic of China for world leadership is intensifying. International competition is intensifying with the use of all instruments of national power – political, diplomatic, military, economic, informational, psychological, and cyber means. Its consequences are manifested in Eastern Europe, the Middle East and North Africa, Southeast Asia, the Arctic, and other regions."

– "To restore its influence in Ukraine, the Russian Federation, continuing the hybrid war, systematically uses political, economic, informational, psychological, cyber and military means. The groupings of the armed forces of the Russian Federation and their offensive potential are being strengthened, large-scale military exercises are regularly conducted near the state border of Ukraine, which indicates the threat of military invasion. The militarization of the territories of the temporarily occupied Autonomous Republic of Crimea and the city of Sevastopol is growing. The threat from the Russian Federation to free navigation in the Black Sea, the Sea of Azov, and the Kerch Strait remains."

In the Military Doctrine of Ukraine, enacted by the Decree of the President of Ukraine No. 555/2015 of September 24, 2015, in paragraph 7, among the main trends influencing the military-political situation in the region around Ukraine, the following is defined:

- "information war of the Russian Federation against Ukraine".

And in paragraph 10 of the Military Doctrine, among the military-political challenges that may develop into the threat of the use of military force against Ukraine, the following is defined:

- "purposeful information (information and psychological) influence with the use of modern information technologies, aimed at the formation of a negative international image of Ukraine, as well as at destabilizing the internal socio-political situation, aggravation of interethnic and interconfessional relations in Ukraine or its individual regions and places of compact residence of national minorities".

Paragraph 17 of the Military Doctrine defines among the main tasks of Ukraine's military policy in the near future and in the medium term, in particular:

- "prevention and effective counteraction to information and psychological influences of foreign states aimed at undermining the defense capability, violating the sovereignty and territorial integrity of Ukraine, destabilizing the internal socio-political situation, provoking interethnic and interfaith conflicts in Ukraine".

In paragraph 32 of the Military Doctrine, Ukraine considers the following main measures and actions as the basis for crisis response to military threats and prevention of escalation of military conflicts, in particular:

- "strengthening intelligence activities in the interests of preparing and conducting strategic communications, counter-propaganda activities and information and psychological operations by Ukraine;
- increasing the effectiveness of special information measures of influence in the area of the anti-terrorist operation in Donetsk and Luhansk regions and in the temporarily occupied territory and concentrating forces and means to organize effective counteraction to the conduct of hostile information and psychological operations against Ukraine".

Thus, within the framework of the Military Doctrine of Ukraine, the need to develop new effective methods to ensure the necessary level of information and psychological protection of people and social groups is determined, including the development of new methods to increase their security, especially in the presence of negative information and psychological influence.

The Cybersecurity Strategy of Ukraine, enacted by the Decree of the President of Ukraine No. 96/2016 of March 15, 2016, states:

– The purpose of the Cybersecurity Strategy of Ukraine (hereinafter referred to as the Strategy) is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state.

To achieve this goal, it is proposed, in particular:

– strengthening the capabilities of security and defense sector entities to ensure effective combating military cyber threats, cyber espionage, cyber terrorism and cybercrime, deepening international cooperation in this area.

The 2021 draft of the Cybersecurity Strategy of Ukraine for 2021-2025 offers [5]:

– strengthen the capabilities of the national cybersecurity system to prevent armed aggression against Ukraine in cyberspace or with its use, neutralize intelligence and subversive activities, minimize the threats of cybercrime and cyberterrorism (deterrence);

– acquire the ability to quickly adapt to internal and external threats in cyberspace, support the sustainable functioning of the national information infrastructure, primarily critical information infrastructure facilities (cyber resilience).

Also, in this project, the main challenges for Ukraine in the field of cybersecurity are:

– active use of cyber tools in the international competition for world leadership, the competitive nature of the development of cybersecurity tools and the implementation of cyber threats in the process of rapid progressive changes in information and communication technologies, cloud computing, 5 G-networks, big data, the Internet of Things, machine learning/artificial intelligence (AI), etc.;

– militarization of cyberspace and the growing technological capabilities of cyber weapons, which make it possible to carry out covert cyberattacks and cyber operations by the enemy, remote control of control systems, damage and destruction of critical information infrastructure;

– growth of the technological level of illegal encroachments on the interests of the state, society and individual citizens with the use of social engineering methods, the use of artificial intelligence technologies and crypto technologies.

Thus, the Cybersecurity Strategy of Ukraine emphasizes the need to protect a person and a social group from negative information and psychological influence using cyberspace.

The standards of the ISO/IEC 27000 – 27037 Information technology – Security techniques series set the requirements for the development, operation and modernization of information security management (ISMS) systems. They are widely used all over the world. For example, in the Russian Federation, their translation is used as a system of standards "GOST R ISO_IEC 27000 – 27037 Information Technology. Methods and Means of Ensuring Security." [1].

The process of developing an information security management system, which is laid down in these Standards, is shown in Fig. 1. On it, a gray rectangle highlights the place of the results that are necessary for its application in practice.

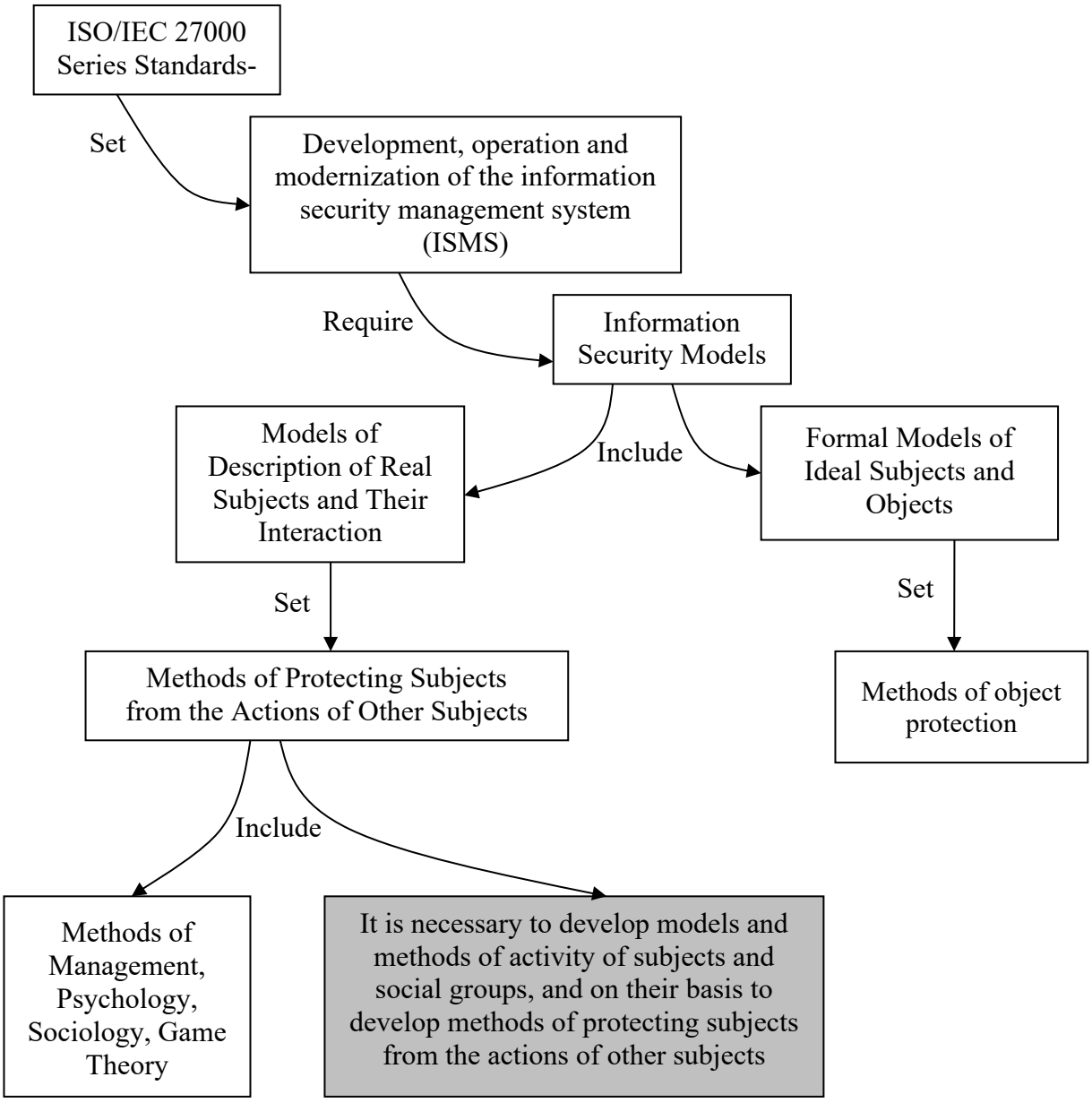

Fig. 1.1. The process of developing an information security management system

The main element of enterprise information security management is ISMS, and the standards of the ISO/IEC 27000 – 27037 Information technology – Security techniques series define the process of its development, operation, audit and modernization.

The application of these standards requires the availability of detailed models of information security. These models fall into two classes. The first class includes formal models of ideal subjects and objects of information security. They are analyzed in detail in the next subsection – it is on their basis that methods of protecting information security objects are built.

The second class of models includes models for describing real subjects of information security and their interaction. Such actors include individuals, structured and unstructured social groups, their interaction both with each other and with the organized social environment.

On the basis of these models, methods of protecting the subjects of information security, including from the influence of other subjects on them, are developed. Today, these methods include methods of management and sociology, psychological methods, as well as game theory [3-38].

However, there is still a great need to develop new models and methods to describe and predict the activities of individuals and social groups (both structured and unstructured). Only on the basis of such models it will be possible to develop models and methods to protect the subjects of information security from negative influence.

Thus, the informational-psychological factors that are used in the process of building models of protection of a person and a social group as subjects of information protection originate from management, psychology, sociology and game theory.

The obvious insufficiency of existing models and methods of protection of individuals and social groups is evidenced by the fact that the WikiLeaks website [2] has several million confidential documents, each of which was voluntarily provided for publication by the very people who were supposed to ensure its confidentiality. Thus, tens (and maybe hundreds) of thousands of people who have access to confidential and secret information have voluntarily violated their functional duties. Moreover, the motivation for such a violation was interaction with other subjects: individuals, structured and unstructured social groups, as well as the environment to which these subjects adapted.

The presence of a growing number of new channels of influence on a person or a social group on the part of other people and social groups leads to the fact that an increasing number of people carry out their activities in conditions of information and psychological influence from other people. The presence of intelligent computer systems, including those with speech recognition and the ability to communicate in a dialogic mode, also lead to the fact that a person assigns information and psychological characteristics to such systems as well.

Thus, today, violations of information security by information security entities in the world are widespread. Moreover, violations of information security through malicious actions against information security objects (for example, hacker attacks) cause much less damage today.

Therefore, the development of new models and methods of information security, focused specifically on the subjects of information security, is an extremely necessary area of activity.

1.2. Modern models and methods of information security management

In modern models of describing information security processes, the subject component – that is, a person or a social group – is modeled at the level of implementation of the given formal rules [7], and these rules relate to both interaction with the objects of information protection and interaction between subjects.

The influence of the subject on the subject is modeled exclusively by formal rules. For example: "subject S_1 activates subject S_2". There are no models for the process of such activation today.

The main axiom of information security modeling is the following: "All information security issues are described by subjects' access to objects" [7].

However, the possibility of one subject influencing another causes the characteristics of the subject to change. In other words, as a result of the influence of another subject, the subject in question ceases to comply with the rules set for it by the information security model.

In modern models of information security, it is assumed that a new subject S_k is generated by a pair (S j,O i), where S_j is another subject and O_i is a certain object.

However, as a result of subject-subject interaction in a cycle, situations are possible when a new subject is generated by two (or more) already existing subjects: $(S_{i,S\,j}) \rightarrow S_k$. For example, it can simply be a change in the state of a particular person as a result of his communication with another. In order to integrate such situations, it is necessary to develop special models both for human activity (for example, due to the fact that different people can perform a given activity in different ways) and for the interaction of people with each other (separately for binary relations between people and for social groups, respectively).

Fig. 1.2-1.4 highlights the following elementary (main) cases of relations between subjects that arise in information security models that describe the functioning of information security management systems (ISMS). There are no models for such elementary cases today, which leads to the inability to correctly assess risks in ISMS.

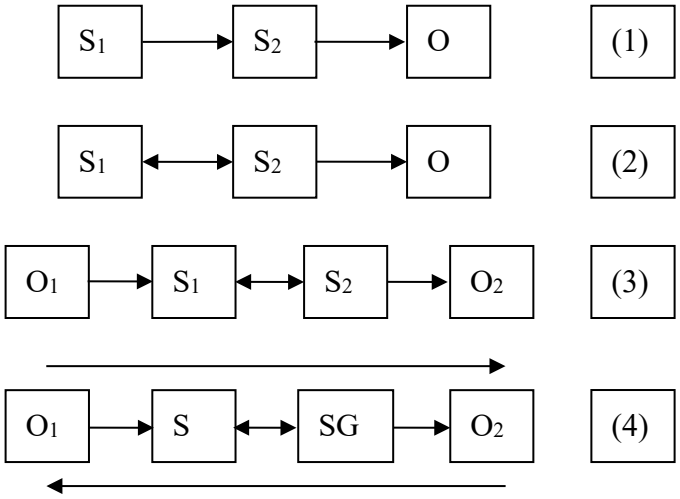

Fig. 1.2. Elementary Subject-Subject Relations in Unstructured ISMS

Fig. 1.2 presents elementary subject-subject relations in unstructured ISMS. Case (1) is characteristic of models of ideal subjects and objects. For example, in the Harrison-Rizo-Ullmann, Take-Grant, and security model synthesis methods, these relationships are assumed to be unidirectional and ideal.

Case (2) describes a situation where there are two entities interacting with each other, as a result of which the characteristics of the second entity may be altered in the course of the functioning of the ISMS.

Case (3) describes a process in ISMS that results in an unauthorized change in a second object.

Case (4) describes a process in ISMS that involves a social group that interacts with an object. The arrows at the top and bottom reflect the fact that a social group can be either the first or second link in the process.

Fig. 1.3 presents elementary subject-subject relations in hierarchically structured ISMS. Fig. 1.2 above and below reflect the fact that the process can go in different directions (from the first subject to the second and from the second to the first).

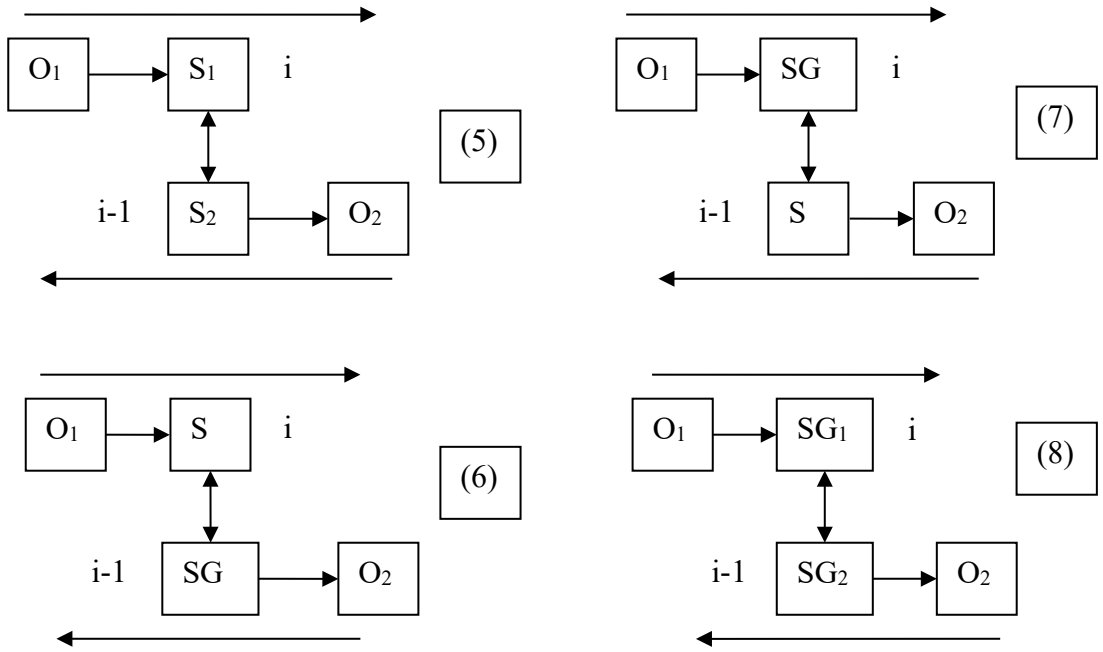

Fig. 1.3. Elementary Subject-Subject Relations
in Hierarchically Structured ISMS

Case (5) describes a process in which two actors are at different hierarchical levels.

Cases (6) and (7) describe processes in which one of the subjects is a person and the other subject is a social group.

Case (8) describes a process in which both subjects are social groups.

Fig. 1.4 describes the process by which an entity is influenced by an entity foreign to ISMS, which can be a person, a social group, or an organized social environment.

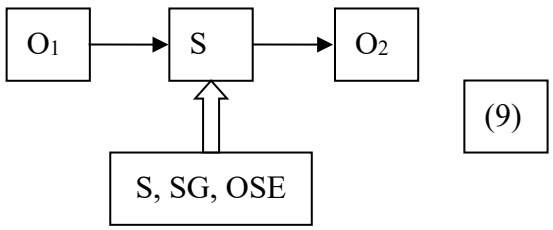

Fig. 1.4. Influence on the subject from the organized social environment
in ISMS

Fig. 1.2-1.4 interaction of subjects can be carried out not only through direct contact, but also through technical means (computers, mobile communications,

gadgets, etc.), and through the Internet and specialized software (social networks, network games, Skype, etc.).

Comparison of the subjective component of information security models. The offender model includes a set of characteristics that describe the impact of a person on the objects of information protection. Thus, the model for the activities of a person or social group is decisive for success.

The situation is similar with models for determining the value of information. The value of information can be determined only and exclusively by the subjects of information protection – people and/or social groups. Moreover, the very concept of the value of information is subjective: different people (social groups) may well provide different value to the same information. In addition, the value of information is different for different activities of a person and/or a social group. Thus, here, too, the presence of a model to describe the activities of a person and a social group is a factor that can increase the security of information.

Following [7], we provide an analysis of the main existing formal models of information security. Only those components of models and methods that describe the subject component are considered, since it is the consideration of the "non-ideality" of subjects and subject-subject relations that is today one of the main sources of reducing the level of protection of a person and a social group.

Privacy Models.

Harrison-Ruzzo-Ullmann model (model of discretionary control (differentiation) of access). It has the following characteristics:

- A complete list of subjects is specified (thereby removing the possibility of the influence of the changing environment on subjects, as well as the removal and replacement of subjects).
- Subjects follow the rules perfectly (thus assuming that all people are 1) the same, 2) do not make decisions based on different circumstances, and 3) deviations from perfection cannot be accounted for in this model).
- Subject-subject relations are ideal and take place (thus it is assumed that they are given and are 1) unchangeable and 2) exactly what is necessary for effective protection of information, 3) deviations from ideality cannot be taken into account within the framework of this model).
- There is no general algorithm for checking security (i.e., it is impossible to take into account the impact of "non-ideality" of subjects and subject-subject relations on the level of security).

Take-Grant access distribution model. It has the following characteristics:

- A complete list of subjects is specified (thereby removing the possibility of the influence of the changing environment on subjects, as well as the removal and replacement of subjects).
- Subjects follow the rules perfectly (thus assuming that all people are 1) the same, 2) do not make decisions based on different circumstances, and 3) deviations from perfection cannot be accounted for in this model).
- Subject-subject relations are ideal and take place (thus it is assumed that they are given and are 1) unchangeable and 2) exactly what is necessary for effective protection of information, 3) deviations from ideality cannot be taken into account within the framework of this model).
- The transfer of access rights is carried out without the assistance of the entity that owns these rights.
- There are theorems for defining graphs in which "information theft is possible" (but it is impossible to take into account the influence of the "non-ideality" of subjects and subject-subject relations on the level of security).

Bella-LaPadula mandate access control model (with McLean and Low-Water-Mark improvements). It has the following characteristics:

- A complete list of subjects is specified (thereby removing the possibility of the influence of the changing environment on subjects, as well as the removal and replacement of subjects).
- Only two access rights are considered: read and write.
- Subjects follow the rules perfectly (thus assuming that all people are 1) the same, 2) do not make decisions based on different circumstances, and 3) deviations from perfection cannot be accounted for in this model).
- There is no subject-subject relationship.
- A theorem for determining the safe state has been proved (but it is impossible to take into account the influence of the "non-ideality" of subjects and subject-subject relations on the level of security).
- The improvements use the level of secrecy of subjects (but it is impossible to take into account the influence of the "non-ideality" of subjects and subject-subject relations on the level of security).

Integrity Assurance Models. Baib's Integrity Model. It has the following characteristics:

- A complete list of subjects is specified (thereby removing the possibility of the influence of the changing environment on subjects, as well as the removal and replacement of subjects).

- Subjects are labeled with a "integrity" indicator that orders them.
- Subjects follow the rules perfectly (thus assuming that all people are 1) the same, 2) do not make decisions based on different circumstances, and 3) deviations from perfection cannot be accounted for in this model).
- There is no subject-subject relationship.
- Monotonous decrease in the integrity of the object (but it is impossible to take into account the influence of the "non-ideality" of subjects and subject-subject relations on the level of security).

The Clark-Wilson Model of Integrity. It has the following characteristics:

- A complete list of subjects is specified (thereby removing the possibility of the influence of the changing environment on subjects, as well as the removal and replacement of subjects).
- Subjects have characteristics similar to those of the Bella-LaPadula and Baiba models.
- Subjects follow the rules perfectly (thus assuming that all people are 1) the same, 2) do not make decisions based on different circumstances, and 3) deviations from perfection cannot be accounted for in this model).
- There is no subject-subject relationship.

Accessibility model.

Millen's Resource Allocation Model. It has the following characteristics:

- A complete list of subjects is specified (thereby removing the possibility of the influence of the changing environment on subjects, as well as the removal and replacement of subjects).
- A subject with a higher level has an absolute right to make inquiries to subjects and objects of a lower level (but it is impossible to take into account the impact of the "imperfection" of subjects and subject-subject relations on the level of security).
- The subject needs the resources of the system to complete the task. Access will only be denied due to insufficient resources. The concepts of "finite waiting time" and "maximum waiting time" have been introduced (but it is impossible to take into account the impact of "non-ideality" of subjects and subject-subject relations on the level of security).
- Subjects follow the rules perfectly (thus assuming that all people are 1) the same, 2) do not make decisions based on different circumstances, and 3) deviations from perfection cannot be accounted for in this model).
- There is no subject-subject relationship.

Methods of synthesis of security models. They have the following characteristics:

- A complete list of subjects is specified (thereby removing the possibility of the influence of the changing environment on subjects, as well as the removal and replacement of subjects).
- Subjects follow the rules perfectly (thus assuming that all people are 1) the same, 2) do not make decisions based on different circumstances, and 3) deviations from perfection cannot be accounted for in this model).
- The subject-subject relationship is connected by the relation of activation. These relations are ideal (thus it is assumed that they are given and are 1) unchangeable, and 2) exactly what is required for effective protection of information, 3) deviations from ideality cannot be taken into account within the framework of this model).

A comparison of models and methods according to the characteristics of the subjects they use is given in Table. 1.1

For all models and methods of information protection, the common characteristics are the following:

- the complete list of subjects is given: thereby removing the possibility of the influence of the changing environment on the subjects, as well as the removal and replacement of subjects;
- all subjects are the same (identical within the same parameter values): the differences between one subject and another (i.e., one person from another) are not taken into account;
- subjects perfectly follow the given rules: thus it is assumed that all people are 1) the same, 2) do not make decisions depending on different circumstances, 3) deviations from ideality cannot be taken into account within the framework of this model;
- it is impossible to take into account the influence of the "imperfection" of subjects and subject-subject relations on the level of security.
- subject-subject relations are ideally executed according to the given rules, thus it is considered that they are given and are 1) unchangeable and 2) exactly those that are necessary for effective protection of information, 3) deviations from ideality cannot be taken into account within the framework of this model;

Table 1.1. Comparative Characteristics of Subjects' Parameters in Information Security Models and Methods (according to [7])

№	Model/Method	Subject Parameters			
		Availability of requirements for the subject	Existence of subject-subject relations	Availability of subject ranking	Model/Method Results
1	Harrison-Ruzzo-Ullmann model	+	+	–/+	There is no common algorithm for checking security
2	Take-Grant model	+	+	–/+	There are theorems to define graphs in which "information theft is possible"
3	Bella-LaPadula model (with McLean and Low-Water-Mark improvements)	+	–/+	+ (McLean and Low-Water-Mark models only)	A proven theorem for determining the safe state
4	Baiba model	+	–/+	+	Monotonic decrease in the integrity of the object
5	Clark-Wilson Model	+	–/+	–/+	Scope – Commercial Companies
6	Millen's model	+	–/+	+	The concepts of "finite waiting time" and "maximum waiting time" have been introduced
7	Methods for Synthesis of Security Models	+	+	–/+	The conditions for the implementation of the security policy have been proven

Thus, the carried out analysis shows that in modern models and methods of information protection, the subject component is clearly represented in an insufficient volume. At the same time, its impact on providing information and psychological protection is growing rapidly over time.

[3-6,31-38] analyzes a wide range of existing models and methods of ensuring the protection of a person or a social group from negative information and information-psychological influence. In particular, it is emphasized that motivational factors have a high level of importance.

Today, the existing channels of influence on a person actively shape his emotional perception of information. As a result, already at the level of perception of information, certain facts will be rejected by it, and certain facts will dramatically change their real priority. Today, negative information and psychological influence on a person is carried out mainly not through the channels of his personal communication, as it was before, but through intelligent information systems (for example, search engines that adapt to a specific person and, thus, change the priority of information).

The use of media channels is widely used (this is especially dangerous for Ukraine, in which the vast majority of TV channels belong to certain oligarchic groups), the Internet (where the owners of web resources bear practically no responsibility for the content), various gadgets of mobile devices, the number of which is growing rapidly (for example, today gadgets actively form the population's emotional attitude to a number of concepts and factors of social life – moreover, Multilingual variants of the same gadget can form opposite emotional assessments among users [39]), etc. The emotional acceptance or rejection of certain factors of social life, formed in this way, has a significant impact on the performance of the individual and the social group.

In modern models and methods of protection of a person and a social group, as a rule, only personal information and psychological characteristics of a person are used, which characterize a particular person, separating him from others [3-38]. This is due to the fact that only psychological models of a person's personality are used as a model of a person. But these psychological models of personality, which are called personality theories within psychology [19], are often used not just heuristic indicators and characteristics, but often even built on the basis of directly opposite assumptions. For example, behaviorists assume that there must be a stimulus first, followed by a person's response [19]. At first glance, this assumption is natural, moreover, this is how modern science is constructed. Indeed, it seems natural that a person reacts exclusively to objective factors of the world external to him. Within the framework of the behaviorist concept, a number of quite effective psychological and psychotherapeutic techniques have been obtained [19]. But the cognitivist concept in personality theory uses the exact opposite assumption: a person carries out activities exclusively in accordance with his subjective perception of the world, and objective factors are often not the main ones for him. Thus, cognitivists look for motivating motives and goals for action in the subjective world of individual ideas and experiences of a person. They have also developed a number of effective psychological and psychotherapeutic techniques [19]. From the point of view of

science, such a situation is impossible: of two opposing assumptions, only one can be true.

In fact, the situation in psychology has developed much more unfavorable for attempts to use its results as elements of models and methods of ensuring the protection of a person or a social group from negative information and psychological influence. Thus, in [19] there are about 15 of the most widespread personality theories in psychology, and all of them differ from each other in a number of parameters.

As a result of the above, it becomes unclear which of these one and a half dozen theories of personality can be used in models and methods of information and psychological security of a person and a social group.

In addition, modern psychology is focused on the study of the personal characteristics of a person. That is, those characteristics that distinguish one person from another. At the same time, for the needs of developing models and methods of information and psychological security of a person and a social group, there is a directly opposite need: it is necessary to move in the opposite direction, namely, to group people according to the factors influencing their activities.

Finally, modern psychology is based mainly on the subjective characteristics of a person, while for the needs of information security of a person and a social group, objective indicators are needed, best of all, related to the results or course of activity of a person or social group.

Therefore, in order to build models and methods of protecting a person or a social group from negative information and psychological influence, it is often necessary to use expert opinions. As a rule, it is often impossible to reconcile them with each other, because they are often heuristic in nature. As a result, the methods obtained with their use to protect a person or a social group from negative information and psychological influence also become heuristic, which significantly reduces the level of protection subjects of the information process.

Thus, there is an urgent need to develop such models of a person or a social group that, firstly, would be based on the objective characteristics of a person, secondly, characterize the course and results of his activities, and, thirdly, create a classification of people according to such characteristics, and this classification should have a relatively small number of classes.

The fulfillment of the first requirement makes it possible to carry out argumentation and verification, which today is almost impossible in the psychological and social models of a person (for example, it is impossible for a behavioral psychologist and a cognitive psychologist to find a common language).

The fulfillment of the second requirement makes it possible to develop methods for protecting a person and a social group from negative information and psychological influence to use those characteristics that are easily observed and can be measured, as well as are accessible and visual to a wide range of people.

Finally, the third requirement will allow you to operate with a relatively small number of protection tools, which will be "configured" on a relatively small number of classes or types.

If earlier social groups were realized in physical space, through direct contact between people, today, thanks to the possibilities of the Internet, social groups often turn into social networks.

The main factors that are taken into account when modeling a person in a social network are the following (recalculation is given using [45]).

1. The presence of a person's own thoughts and aggregated opinions in a social group.

2. The significance of the opinions of one person or a particular social group on another person or social group is different in influence.

3. Different degrees of susceptibility to outside influences for a person or social group.

4. The existence of indirect extraneous influence on a person or social group and the presence of a decrease in the magnitude of such influence depending on the "psychological and/or social distance" from the source of influence.

5. The existence of "opinion leaders" and essay groups whose opinions and influence take significant precedence over the opinions and influences of other people and social groups.

6. The existence of a threshold of sensitivity to changes in the opinions of people and social groups around them.

7. It is preferable to group people into a single group with people who share the same opinions.

8. The presence of specific social norms and the grouping of people according to the uniformity of these norms.

9. The need to take into account the so-called "social correlations", that is, the presence of "typical behavior" that is characteristic of people from a given social group.

10. The existence of external factors of influence and external factors of information influence – for example, the media.

11. The presence of specific and characteristic stages in the dynamics of change of opinion in a person or a social group, for example, the diffusion of innovations, etc.

12. Avalanche-like effects, where a change in a person's or social group's opinion has a threshold effect.

13. The influence of structural characteristics of a social group, for example, the number of connections of an individual in it, the presence of clusters with an increased number of connections, the length of the chain of distribution of opinions in a social group, etc.

14. The presence of purposeful behavior of a person in a social group.

15. Ability to create coalitions in a group.

16. The impact of incompleteness and/or asymmetry of information possessed by a person (individual or in a social group) on his/her activities.

17. Decision-making by a person or social group in conditions of incomplete information.

Today, there are many models for determining the value of a social network, in which the term "value" is defined as the number of connections between people in that group.

For example, the so-called "Metcalfe's Law" states that the value of a social group increases as n^2 [45-47]. This is explained by the fact that the number of binary bonds between n elements is

$$V = \frac{n(n-1)}{2}. \tag{1.1}$$

Attempts to take into account not only binary relationships have led to the following formula for determining the value of a social group:

$$V = 2^n - n - 1. \tag{1.2}$$

This relationship is called "Reed's law" and is computed as the number of subsets in a set of n elements, excluding single elements and an empty set.

In general, combining Metcalfe's Law and Reed's Law, and taking into account that some of the connections may be missing, we get the following formula

$$V = a \cdot 2^n + b \cdot n^2 + c \cdot n. \tag{1.3}$$

Other expressions for the value of a social group have also been proposed, such as the following

$$V = n \cdot \ln n. \tag{1.4}$$

However, it is known from many numerous observations and experiments that people in a social group never create the maximum possible number of bonds. Today, there are no models that could explain this phenomenon.

Finally, the value of a social group cannot be reduced to the number of connections between people alone. In addition, there are hierarchically organized social groups, for which completely different characteristics will be important.

It is also important to emphasize that it makes sense to consider models for an individual or for a social group within the framework of information and psychological security only within the framework of describing their activities and third-party influence on these activities. This is due to the fact that negative informational-psychological influence is aimed, in the final sense, at the only and only deterioration of the activities of both an individual and a social group.

In [6] it is proposed to allocate the following directions for studying the problem of information influence, information management and information confrontation:

1. informational influence on an individual, social and other groups, society as a whole;
2. targeted influence (information management), in particular with the help of the media;
3. the struggle for information influence and the formation of the necessary public opinions;
4. the impact of information on the security of management decisions made on the basis of this information;
5. information confrontation (including covert) at the interstate, national, regional, territorial, sectoral and corporate levels.

In [6] it is noted that these areas of research have not yet attracted a wide range of researchers, even despite their importance.

Unfortunately, in modern studies of social groups, the main attention is paid to the analysis of social ties between people. At the same time, the reasons for the establishment of such connections are still left to the attention of researchers.

Table 1.2 provides a comparison of existing methods of protecting a person or a social group from negative information and psychological influence. It also sets out the requirements for those methods of protection of information security entities that are necessary for the successful operation of the ISMS.

Table 1.2. Comparison of existing methods of protecting a person or social group from negative information and psychological influence. The comparison is made according to the characteristics of the subject.

№	**Name of methods to describe a person or social group**	Maslow's hierarchy of needs	McClelland's Theory of Needs	Herzberg's two-factor theory	MacGregor's Theories X and Y	Vroom's Theory of Expectations	Porter-Lowther model	Levin's Leadership Styles	Leucart's Leadership Styles	Conflict Theory	Moreno's sociometrics	Kretschmer's typology	Sheldon's typology	Jung's typology	Mayer-Briggs typology	Cattell's typology	Eysenck's typology	**Required Models and Methods**
	Characteristic Name																	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	**19**
1	What is the object of the method:																	
	– Individual	+	+	+	–	+	+	+	+	–	–	+	+	+	+	+	+	+
	– Social group	–	–	–	+	–	–	–	–	+	+	–	–	–	–	–	–	+
2	A human model is required to apply the method	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–
3	The method incorporates a human model	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
4	The method is applied to:																	
	– Individual	+	+	+	+	+	+	+	+	–	–	+	+	+	+	+	+	+
	– Social group	–	–	–	–	–	–	–	–	+	+	–	–	–	–	–	–	+
5	The method uses the following characteristics:																	
	– Individual	–	–	–	–	–	–	–	–	–	+	–	–	–	–	–	–	+
	– Social group	–	–	–	–	–	–	+	+	+	–	–	–	–	–	–	–	–
	– All people	+	+	+	+	+	+	–	–	–	–	+	+	+	+	+	+	–
6	The method uses the characteristics of the subject areas:																	
	– Psychology	–	–	–	–	–	–	–	–	–	–	+	+	+	+	+	+	–
	– Sociology	–	–	–	–	–	–	–	–	–	+	–	–	–	–	–	–	–
	– Management	+	+	+	+	+	+	+	+	+	–	–	–	–	–	–	–	–
	– Performance Results	–	–	–	–	–	–	–	–	+	–	–	–	–	–	–	–	+

Continuation of the table

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	**19**
7	Level of justification of the method:																	
	– Causal	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
	– Statistical	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+	+	–
	– Empirical (expert)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	–	–	–
8	Level of verification of the method:																	
	– Causal	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
	– Statistical	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+	+	–
	– Empirical (expert)	+	+	+	+	+	+	+	+	–	+	+	+	+	+	–	–	–
	– Forecast and its verification	–	–	–	–	–	–	–	–	+	–	–	–	–	–	–	–	+
9	The method allows you to identify leaders and talents	–	–	–	–	–	–	–	–	–	+	–	–	–	–	–	–	+
10	The method makes it possible to make a forecast in conditions that are new for a person or a social group	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
11	The results of the method can be used in other methods	–	–	–	–	–	–	+	+	+	+	–	–	–	–	–	–	+
12	The method allows you to predict the results of activities:																	
	– Individual	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
	– Social group	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
13	Information about a person allows you to predict:																	
	– Binary relationships between people	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
	– Structures in a social group	–	–	–	–	–	–	–	–	–	+	–	–	–	–	–	–	+
	– Hierarchy of the social group	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+
14	Allows to predict the impact on a person or social group of their social environment	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	+

1.3 Method of detecting threat agents in cybersecurity tasks

The Cybersecurity Strategy of Ukraine states: "The purpose of the Cybersecurity Strategy of Ukraine (hereinafter referred to as the Strategy) is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state" [1]. Paragraph 4.1 also states: "The development of a secure, stable and reliable cyberspace should consist primarily of: ... creation of a system for timely detection, prevention and neutralization of cyber threats, including with the involvement of volunteer organizations;

Thus, in accordance with the Cybersecurity Strategy of Ukraine, a wide range of information security entities should be involved in ensuring the information security of an enterprise. The same is stated in the modern information security standards of the ISO/IEC 27000-27037 series Information technology – Security techniques.

The Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" provides the following definition: "Cybersecurity is the protection of the vital interests of a person and a citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace."

The study of quantitative values of indicators of informal communications that affect the protection of confidentiality is necessary both for use in the development of models and methods of information security, and for their verification. In addition, such quantitative results can be used as normative values in the context of the development and design of privacy protection systems, taking into account the specific characteristics of a particular object of protection.

Thus, the study of indicators of informal communication in socialnetworks to identify agents of privacy threats is an important area for scientific development, which can often be critically important for ensuring the information security of protection subjects.

The characteristics that are promising for use in informal communication studies to identify threat agents are based mainly on management and personnel management [2–5]. Unfortunately, they often use psychological or sociological methods that require direct communication with the subject of threats. This leads to an increased risk that such characteristics will not be detected as a result of the

concealment of information by the investigated entity — the agent of confidentiality threats.

There are not so many quantitative indicators that are the most informative for the tasks under consideration. Among them, sociometric indicators proposed by J. Moreno in the late 1950s stand out [6]. The carried out studies have revealed that these indicators can be effectively applied in the conditions of enterprises in Ukraine [7]. But the fundamental flaw in the use of existing information technologies [8, 9] is the need to interview threat agents, which makes it impossible both to promptly obtain the necessary information and to monitor it concealed from threat agents. In [10] a method of generalization of sociometric indicators using social networks is proposed.

Today, research on social networks focuses mainly on modeling the aggregate indicators that characterize such networks [11]. At the same time, agents are often relied on to be the same. Recently, however, there has been a growing number of studies aimed at identifying influencers on social networks: these results are extremely important for the problem of diffusion of innovations or the identification of agents of influence. For example, in [12], a sociogram of 11 people was used as a tool, in which each of the 195 subjects was asked to imagine themselves in this group, determine a position for themselves, choose another element for interaction, and predict their probability of fulfilling the requests of another agent.

In [13] a method for determining the social role of agents in social networks is proposed, which is used for Facebook and Wikipedia. This method is based on the fact that it assumes the existence of roles in advance, which limits the scope of the results obtained.

In [14] a number of models of formation of social networks are considered, the task of which is to illustrate how the desire of agents to transmit information (that is, to establish connections with other agents) contributes to their diffusion of information across the network. The main focus of the study was on the formation of cyclical structures from agents in the social network.

Thus, the existing methods and tools for their implementation do not provide a complete and anonymous study of communication in social networks for agents, which limits their application to the task of identifying agents of confidentiality threats and creating a cyberspace that is safe for humans and society.

The aim of the article is to study the indicators of informal communication in social networks to identify agents of privacy threats obtained using the developed software based on the method proposed in [10].

The paper uses the method [10], since it, unlike the existing ones [6–9], does not require a survey of potential threat agents. This makes it possible both to avoid informing subjects about their inclusion in the set of potential privacy threats, and to monitor the indicators that characterize their potential danger.

Let's briefly describe this method for the case of such social networks, which use only positive reviews ("likes") of some agents towards others. The method can be presented in the following form.

Stage 1. A set of H employees who can potentially be threat agents is formed.

Stage 2. For each i -th agent, a set of $R_{i\to j}$ likes is formed, which he gave to each j-th agent.

Stage 3. For each i-th agent, there is a set of $R_{i\leftarrow j}$ j likes that he received from each j-th agent.

Stage 4. For each i-th agent the following formula

$$P_{i\to} = \frac{1}{(N-1)} \sum_{j=1, j\neq i}^{N-1} R_{i\to j} \tag{1.5}$$

Calculates the number of likes with which this agent marked the posts of all other agents of influence in the enterprise. Here, the total number of agents of influence is denoted by N.

Stage 5. For each i-th agent the following formula

$$P_{i\leftarrow} = \frac{1}{(N-1)} \sum_{j=1, j\neq i}^{N-1} R_{i\leftarrow j} \tag{1.6}$$

Calculates the number of likes with which posts of the i-th agent were marked by all other agents of influence.

Stage 6. Using formulas (1) and (2) for each i-th agent of influence, we calculate the "reciprocity coefficient" using the following formula:

$$M_i = \frac{P_{i\leftarrow}}{P_{i\rightarrow}}. \quad (1.7)$$

Stage 7. Order the values of M_i in descending order of numerical values. Lower values correspond to the fact that the threat agent is trying to participate in the communicative activities of the group, but the group does not perceive him as "important" or "significant" to the group person. It is these threat agents who have the lowest level of motivation to maintain confidentiality, constantly being in conditions of actual isolation from other agents. And that is why, over time, they will value the opinion of the team the least. Therefore, those threat agents that are at the beginning will pose a threat to the confidentiality of information. Thus, at this stage, a rating of agents who are motivated to generate privacy threats is created.

Stage 8. There are 5-9 agents that have the lowest values of the reciprocity coefficient (or 10% of agents when the number of threat agents N is large enough), which will make up the set of T agents of confidentiality threats, in respect of which it is necessary for information security and personnel management structures to work together to increase the level of adaptation to communication in the team of these threat agents.

In order to be able to use this method to study the indicators of informal communication in social networks to identify agents of privacy threats, it is necessary to develop a tool (namely, software) for its implementation.

The algorithm for implementing the method in the form of a computer program for the social network Meta (Facebook) is as follows.

1. Accounts are added to the program (using public IDs of users of the social network Meta (Facebook).

2. Accounts are grouped into a group that will be investigated in the future.

3. For each user of the group, their personal posts from the wall are downloaded via API networks.

4. The last post from the wall, which is contained in the program database, is checked with the list received from the API.

5. Wall posts that are missing are added to the general list.

6. For each user of the group, information about likes on personal posts is uploaded via API networks (based on the data on the posts on the wall collected earlier).

7. Each post is analyzed: if there are users of the studied group from the list of users who liked this post, the information about the liked is recorded in the database.

8. After collecting all the data, when the group is displayed, the data on likes is sorted according to the given user.

9. For each user, formulas (1) and (2) determine the coefficient of reciprocity "I to the group" and "Group to me".

10. For each user, the reciprocity coefficient is determined by formula (3).

11. Users are ordered in descending order of reciprocity coefficient.

The project is implemented using the ASP programming language.NET MVC using a specific form of Inversion of control (IoC) — Dependency Injection, namely its implementation Ninject Framework. Work with the database is provided by the Entity Framework technology. To work with the open API of the social network, the implementation of sending/receiving requests from the server has been implemented. The Chartjs library is used to display charts. The Chartjs library is used to display the charts. User authorization is performed by means of network Meta (Facebook).

The UML-structure of project dependencies for the algorithm is shown in Fig. 1.

The algorithm implementation project consists of 9 subprojects.

The Sociality.Presentation project is responsible for displaying data in the browser, which consists of controllers where the data for display is processed, data models and the display itself.

The process of user authorization is handled in the project Sociality.Authorization. User authorization takes place using the social network network Meta (Facebook), so only users who are registered in this network will have access to the program.

Work with the social network is provided by the project Sociality.Helpers: it implements requests to the network's API and processes responses (the request format is Json).

Three projects are used to work with data: Sociality.Core, Sociality.Data and Sociality. The first describes all the implemented tables of the database used by the program in the form of classes. The second is responsible for connecting the program to the database, it contains a description of all dependencies in the tables, and it is also responsible for changes in the structure of the database that may arise in the process of work (the so-called migrations). Well, in the third project, general methods of working with data are implemented, uch as: get a table item by ID, change or delete it, etc.

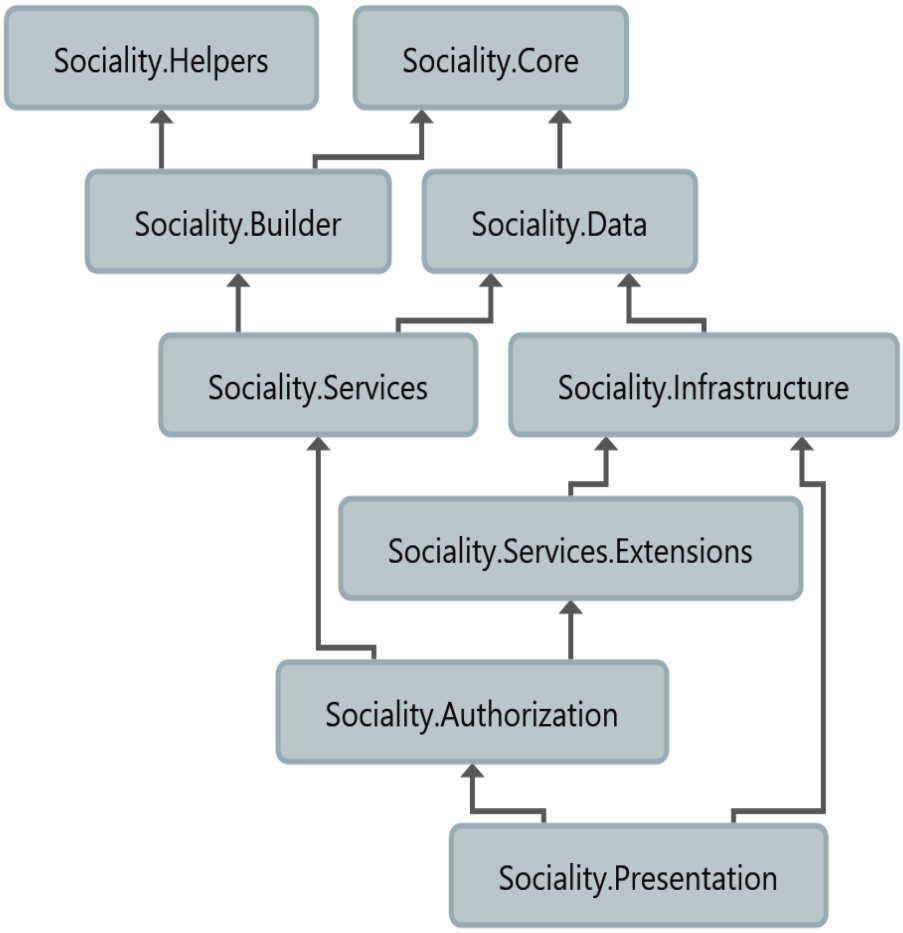

Fig. 1.5 UML structure of project dependency

To display data, additional models with this data are usually used, which are formed in the class Sociality.Builder. Since the project is built by means of dependencies, for all projects to access the settings of this dependency, they were moved to the project Sociality.Infrastructure, and Sociality.Services.Extensions additionally contains the main parameters for working with services.

The UML structure of the database relationship is shown in Fig. 1.6.

The project database consists of 9 tables. After successful registration, through the OAuth mechanism, the program receives data about the user — his address, full name, nickname, phone number, etc. For different user roles in the system (for example, administrator, moderator, SEO specialist, etc.), there is a Roles table, and since a user can have several roles at the same time, the UserRoles relationship table is designed. Authorization is implemented using the social network Meta (Facebook), this is recorded in the UserLogins table — from which social network the user logged in.

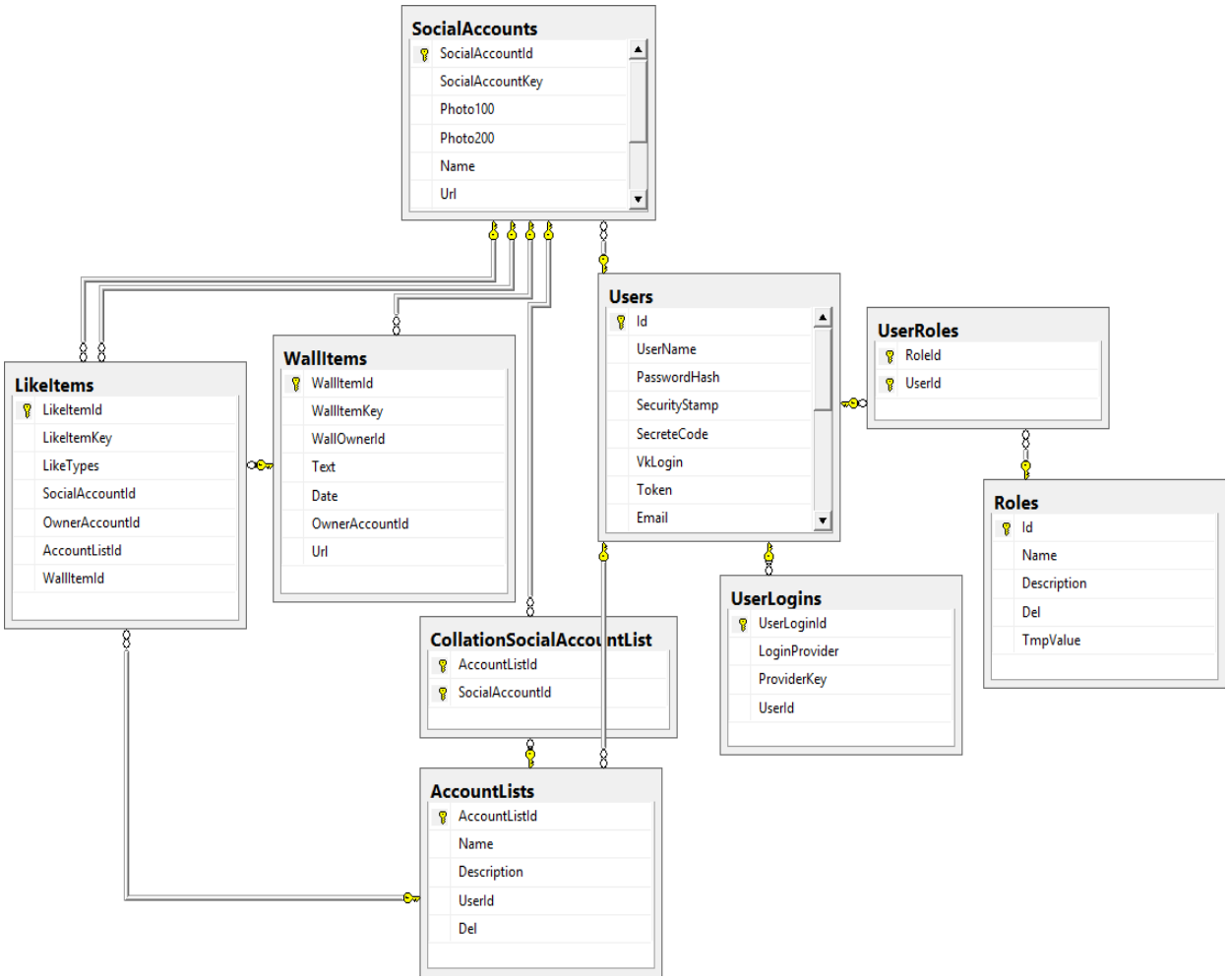

Fig. 1.6. UML Database Table Relationship Structure

When an authorized user adds certain accounts from the network to the program using a public nickname, the program receives data about the user through API networks and enters it into the SocialAccounts table.

When the user combines the previously formed accounts (elements of the SocialAccounts table) into the group to be analyzed, an entry is created in the AccountLists table for the created group (its name, short description) and the accounts that belong to it are added to the account association table with the CollationSocialAccountList group. A separate relationship table is created between the account and the CollationSocialAccountList group Since it should be assumed that one account can belong to several groups.

After creating a group, the data on the posts on the social network wall is recorded/updated in the WallItems table, and the data on the likes received on the network is recorded in the LikeItems table.

The main menu of the authorized user is shown in Fig. 1.7. With its use, the user can create separate groups consisting of different agents (i.e. different accounts).

Fig. 1.7. The main menu of the authorized user.

An academic group of students was selected for the study, which consisted of $N = 26$ people. All students are members of the social network Meta (Facebook). In order to preserve personal data, the names of students are omitted.

Fig. 1.8 shows the distribution of the number of likes received for each agent in the selected group. The program also allows you to present in a separate window the distribution of the number of likes that each of the agents of this group gave to other agents.

In all figures and in the table given in the article, the names of the agents are covered for confidentiality.

As you can see, in this social group, the likes received are unevenly distributed. There is a group of subjects to whom the group practically does not pay attention. A group of subjects that are in the circle of interests of a social group is also allocated.

The program also allows you to present the results in the form of a pie chart (Fig. 1.9), which increases the clarity of the presentation of materials. This chart shows the relative number of likes that a social group provided to a dedicated agent, calculated using formula (2). The numerical values of the corresponding indicator are shown in the table.

Fig. 1.8 shows that four agents ("Natasha", "Veronica", "Marina" and "Dima") are given a lot of attention by this social group, and the quantitative values of the indicator that characterize this attention do not differ much (see Table).

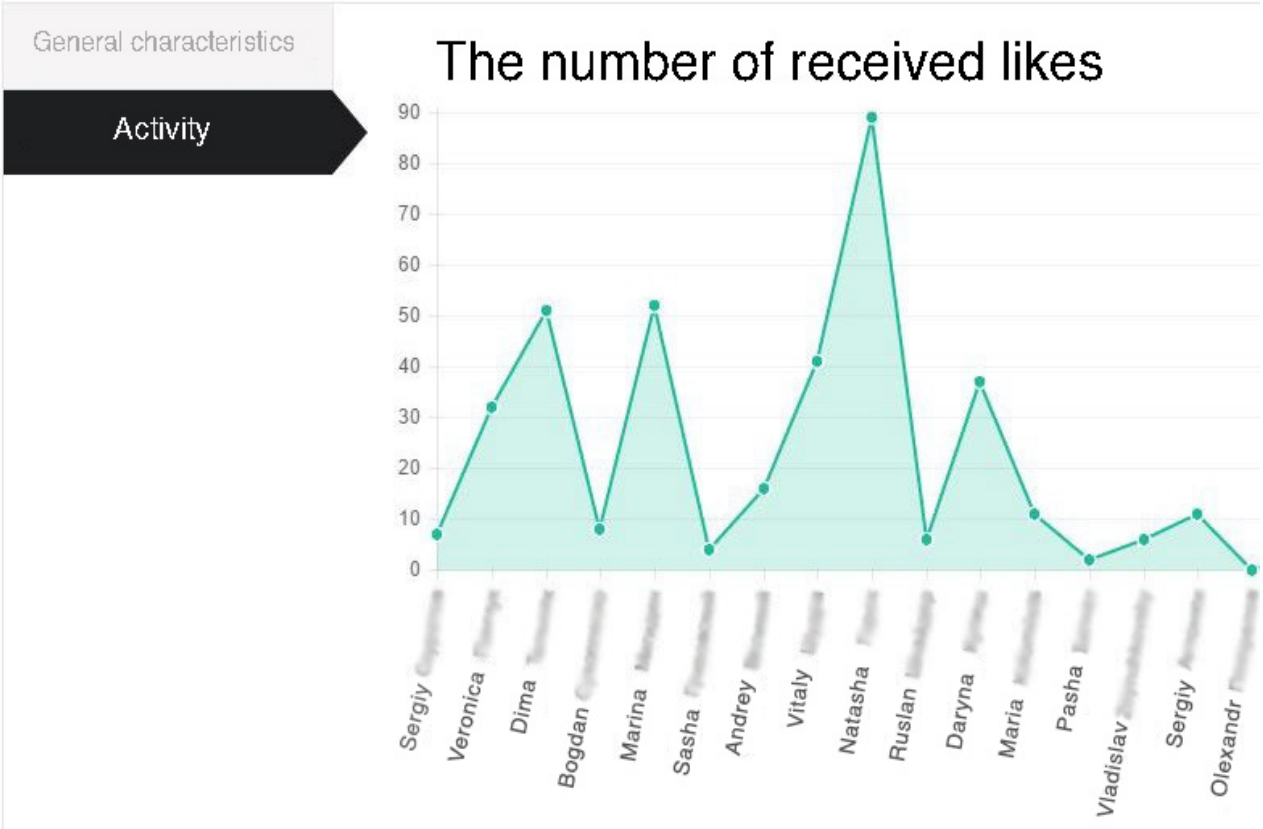

Fig. 1.8. Distribution of the number of likes received for each agent from the selected group.

To analyze both the likes received and provided by each of the agents, calculations are made in the computer program according to the formulas (1), (2) and (3). The results of the relevant calculations are shown in Fig. 1.10, which lists only a subset of agents.

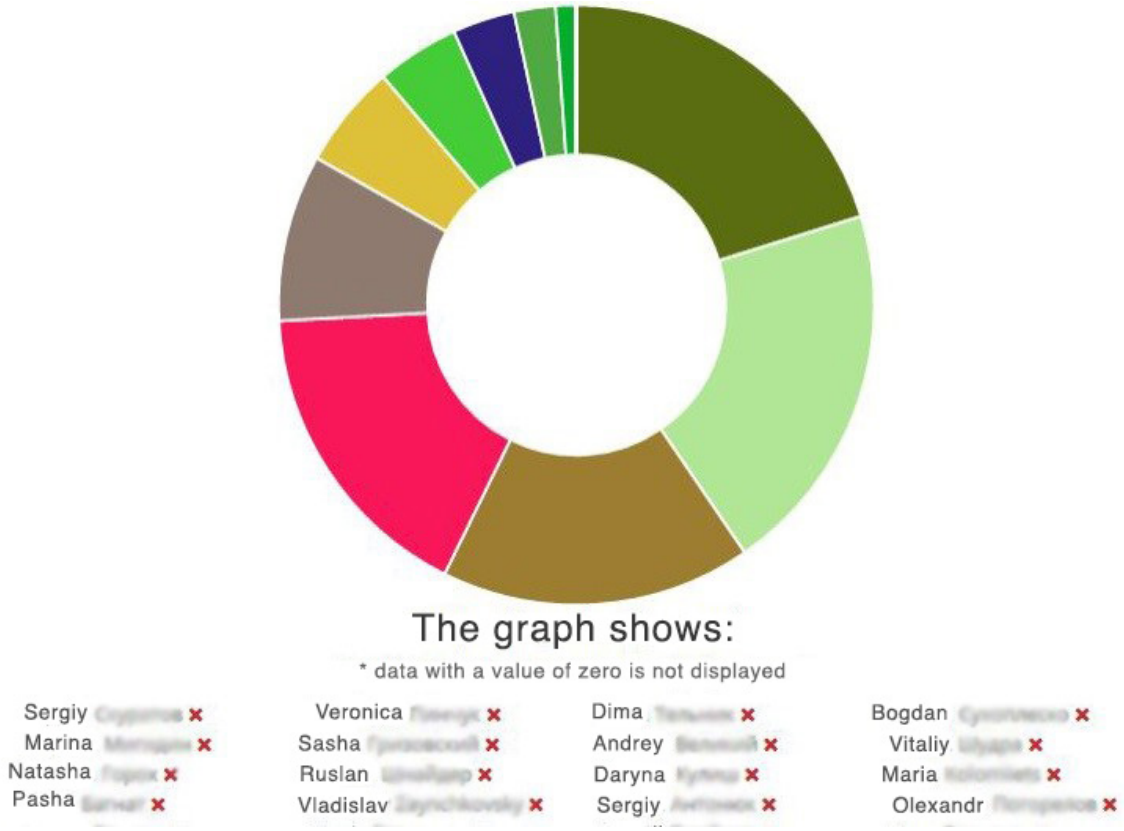

Fig. 1.9. Graphical representation of the distribution of the number of likes, with which the social group marked the posts of a given agent

Coefficient of reciprocity

those groups that did not put and did not receive likes are marked in red

those groups that posted and did not receive likes or vice versa are marked in yellow

Account	Group to the account	Account to the group	Coefficient
Ivan	1,60 (40 likes)	0,08 (2 likes)	20,00
Andrey	1,12 (28 likes)	0,24 (6 likes)	4,67
Sasha	0,16 (4 likes)	0,04 (1 likes)	4,00
Michael	0,12 (3 likes)	0,60 (15 likes)	0,20
Olexandr	0,00	0,00	--
Sasha	0,00	0,00	--
Maxim	0,00	0,24	--

Fig. 1.10. The results of the calculation of the values $R_{\leftarrow}$, $R_{\rightarrow}$ and M_i (only a part of the results are given, as they occupy two windows on the screen)

Table 1.3 shows all the results calculated by computer software for the quantitative values of coefficients (1)–(3).

Table 1.3 Results of calculations of $R_{\leftarrow}$, $R_{\rightarrow}$ values and $_{M_i}$ and ordered by decreasing the value of the reciprocity coefficient $_{M_i}$

№	Account	Group to acanthus $R_{\leftarrow}$	Group Account $R_{\rightarrow}$	Coefficient M_i
1	Ivan	1,60 (40 likes)	0,08 (2 likes)	20,00
2	Andrey	1,12 (28 likes)	0,24 (6 likes)	4,67
3	Sasha	0,16 (4 likes)	0,04 (1 likes)	4,00
4	Dima	2,12 (53 likes)	0,64 (16 likes)	3,31
5	Natasha	3,64 (91 likes)	1,56 (39 likes)	2,33
6	Sergiy	0,44 (11 likes)	0,20 (5 likes)	2,20
7	Andrey	0,16 (4 likes)	0,08 (2 likes)	2,00
8	Maria	1,40 (35 likes)	0,72 (18 likes)	1,94
9	Vitaliy	1,68 (42 likes)	1,08 (27 likes)	1,56
10	A B	1,12 (28 likes)	0,76 (19 likes)	1,47
11	Eugene	1,04 (26 likes)	0,88 (22 likes)	1,18
12	Sergiy	0,32 (8 likes)	0,36 (9 likes)	0,89
13	Veronica	2,24 (56 likes)	2,56 (64 likes)	0,88
14	Bogdan	0,72 (18 likes)	0,88 (22 likes)	0,82
15	Vladislav	0,32 (8 likes)	0,44 (11 likes)	0,73
16	Andrey	0,64 (16 likes)	1,00 (25 likes)	0,64
17	Marina	2,28 (57 likes)	4,20 (105 likes)	0,54
18	Maria	0,96 (24 likes)	2,04 (51 likes)	0,47
19	Daryna	1,48 (37 likes)	3,56 (89 likes)	0,42
20	Pasha	0,08 (2 likes)	0,24 (6 likes)	0,33
21	Bodia	0,12 (3 likes)	0,40 (10 likes)	0,30
22	Ruslan	0,40 (10 likes)	1,36 (34 likes)	0,29
23	Michael	0,12 (3 likes)	0,60 (15 likes)	0,20
24	Olexandr	0,00	0,00	–
25	Sasha	0,00	0,00	–
26	Maxim	0,00	0,24	–

Thus, for a given social group, the agents of privacy threats can be "Michael", "Alexander", "Sasha" and "Maxim".

From the presented results, the following general conclusions can be drawn.

Firstly, more than half of the studied social group, the quantitative values of the reciprocity coefficients M_i of which exceed 0.7–0.8, feel quite comfortable in interaction with the group.

Secondly, there is a relatively small subgroup of eight agents, the level of activity of which in the group is quite high (the quantitative values of the $R_{\rightarrow}$ coefficient of which exceed the average value for the group of 1.00).

Thirdly, a subgroup of 11 agents is singled out, the attention to which is predominant among the members of the group (the quantitative values of the $R_{\leftarrow}$ coefficient of which exceed the average value of 1.00 in the group). As you can see, the group is interested in the activities of almost half of its agents.

Fourth, there is a subgroup of two agents who do not interact with the social group at all. These agents can pose a privacy risk, as they do not value their communication with the social group, and the group does not seek to communicate with them.

The developed tool (computer program) has proven its prospects of use as a tool for detecting agents of confidentiality threats.

Unlike the existing software products [8, 9] and the methods used in a number of studies [12], the tool proposed in the article does not require direct communication with agents. This allows it to be used as a tool for covert analysis of the situation in a given social group. This is especially important for the tasks of ensuring the protection of confidentiality, since existing computer tools can, firstly, scare the attacker and, secondly, the attacker, knowing about the analysis, can provide distorted data.

Within the framework of the proposed computer program, it is possible to allocate agents of influence on the social network as persons who have the highest numerical values of the $R_{\leftarrow}$ coefficient. This makes it possible to apply this program to the tasks and problems discussed in the articles [12–14]. As a result, the proposed computer program can be applied to a wide range of tasks such as modeling social networks [11, 14] and to increase their protection from leakage of confidential information.

1.4. Conclusion to Chapter 1

1. The National Security Strategy of Ukraine, the Military Doctrine of Ukraine, the Cybersecurity Strategy of Ukraine and other documents emphasize the growing need to strengthen measures to protect a person and a social group from negative information and informational-psychological influence, the need to develop new methods and means for the implementation of this activity.

2. It is shown that in modern models of description of information security processes, the subject component (a person or a social group) is modeled at the level of implementation of the given formal rules, and these rules relate to both interaction with objects of information protection and interaction between subjects. It is shown that there is a need to develop such models of activity of subjects and subject-subject interaction, which allow to carry out formal modeling.

3. The existing models of management of subjects are analyzed. It is shown that for the tasks of information and psychological security there is a need to develop new models of human activity and human interaction, since the existing models cannot be effectively used.

4. The proposed tool is a promising tool for identifyingagents of confidentiality threats in the case when agents are part of a social network.

5. Grouping of quantitative values of coefficients, $R_{\leftarrow}$, $R_{\rightarrow}$ and M_i allows to analyze information processes in the social network, to identify informal agents of influence on the network and agents that are ignored by the network, and those agents who actually ignore the activities of the network (almost without taking part in its activities).

6. The proposed remedy is used without the participation of agents of the social network, which excludes the distortion of the research results, since the channel of uncontrolled influence on the social network is excluded. This increases the level of reliability of the data obtained.

7. The proposed computer program is a powerful tool for monitoring social networks, as it can be used even in the background. This allows you to get the dynamics of the coefficients $R_{\leftarrow}$, $R_{\rightarrow}$ and M_i in its temporal unfolding. In particular, it allows you to detect agents that become a potential privacy threat in time.

Thus, there is a need to increase the protection of a person and a social group from negative information and psychological influence through the development of models, methods and means of protecting subjects and various kinds of subject groups in need of protection, taking into account the characteristic features of the activities of both individual subjects and as part of a social group, as well as the features of binary relations between these subjects.

CHAPTER 2 FORMATION OF INFORMATION SPACE IN THE TASKS OF INFORMATION SECURITY AND CYBERSECURITY

2.1 Universal operators of informationspace

For the tasks of protecting a person or a social group as a subject of information protection from negative information and psychological influence, it is important to identify the goals of such influence, which are the ways of perception and processing of information inherent in a person or social group.

The main feature of the perception and processing of information by the subject of information protection is the creation of the information space of the task, which is focused on decision-making and the implementation of activities by a person or a social group.

Let us emphasize the important difference between this term and those that were previously used in the field of information security or information warfare [33]. In these works, the definition of the concept of "information space" was not given, and the methods of its construction were not developed. In fact, the term was used as a metaphor, which clearly reduced the possibilities of its use.

It is possible to introduce a subjective and objective definition of information and information space. The subjective definition of these terms is one that cannot be communicated to other people in order for them to take advantage of it. Such a definition exists only within the subjective space (psyche) of an individual and cannot be subject to translation, i.e. the transfer of its content to another person without distortion (see cognitive psychology, in particular [19,56,57]).

The objective definition of the terms "information" and "information space" is focused primarily on the fact that its content can be broadcast, i.e. transmitted to other people without distortions of content. This is exactly what is required within the framework of technical science.

Within the framework of the general approach to the formation of technical sciences [36,40], it is required that such a definition be constructive. By this, it is understood that the definition itself should include a method (algorithm, technology, method, etc.) in order to be able to build exactly the object that is being defined.

Therefore, the information in the dissertation will be understood as parameters and characteristics (data) that are objective and that relate to a given task. This data can be both quantitative and qualitative. They can also express the results of expert analysis (e.g., after summarizing them by methods [58]).

From a general point of view [36,40], each subject of information security compresses information describing a certain task in order to be able to benefit from the experience of both other subjects and their own previous experience. Thus, each subject that perceives information, makes a decision or carries out an activity first classifies this information. In the process of such classification, some part of the information is rejected as such that describes only a specific entity or event – for this part of the information it is impossible to use previous experience (it, however, may well be generalized and analyzed in the future).

Since the late 1990s, much of the attention of researchers in the field of information technology has been focused on such a mathematical object as ontology. The term "ontology" in information technology refers to a specific type of information about an object or a computable artifact [59-63], i.e. a specific classification of parameters and characteristics. This simply refers to a pragmatic desire to use modern computer capabilities to help a person improve the efficiency of his activities. However, we will use the term "information space", which is familiar to the tasks of information security of the state [4-7,33].

In the existing approaches to the construction of information space (as well as ontologies) there is an implicit assumption. It consists in the fact that the construction of the information space is considered as the construction of a certain "absolute" structure, which "absolutely" corresponds to the formal model of the structure of the system (that is, the structure of the subject area).

This assumption is not fair for a number of reasons. First, it is impossible to construct an "absolutely adequate" formal model of the object under study. For example, the growth of scientific knowledge (which is "necessarily" formalized) will constantly lead to the need for constant changes in the previously built information space (ontology): new objects and new connections between them will appear.

Secondly, the very "filling" of the subject area (definition of classes, their hierarchy, definition of properties of classes and their permissible values, filling in the values of parameters and characteristics) depends on the goal that is set for the subject carrying out the activity.

Thus, taking into account the purpose of building an information space is crucial for its optimal use. Moreover, the goal of constructing an "ideal" (or "complete") information space for a given task, as shown above, cannot be achieved at all. And vice versa, the formation of an information space focused on the given interiors of practical activity has a high potential for practical application.

The proposed approach to the formation of the information space in graphical form is shown in Fig. Figure 2.1, which reflects the main stages of modeling and the formation of a concept based on it [43,53,64-66].

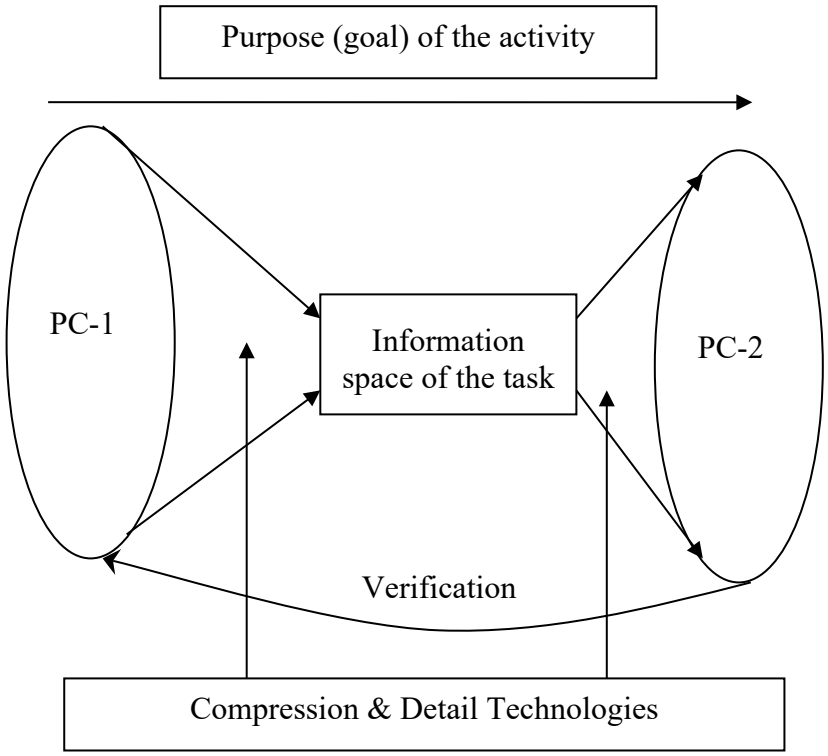

Fig. 2.1. Graphic representation of the scheme of formation of the information space

Initially, for a given task on information security, a goal is formed, which is set by the target components of the set, which sets the activities of the corresponding subject of information security. In accordance with this goal, a set of parameters and characteristics of the real world (PC-1), which relate to the subject area of the task, is considered. Then, using the methods of information compression, the transition from the real world of PC-1 to the "model world" (MS), i.e. the information space itself, which is necessary for the implementation of activities in the subject area, is

carried out. MC elements are treated as abstract symbols and characteristics. At the same time, it should be taken into account that such "compression of information" can be carried out – even within the same task – in several different ways (each of which depends on the purpose of the activity). As a result, several different information spaces for the same task are obtained. Such a situation, for example, is quite typical when constructing ontologies [59-63,65].

At the second stage, there is a solution to the problem within the framework of the received information space. As a result, a solution(s) is obtained, which is focused on a whole class of specific problems.

At the third stage, the solution obtained within the information space is filled with the information content of a specific task. In fact, using the methods and technologies of detailing, a "reverse" transition is made to specific values of parameters and characteristics related to a given subject task and corresponding to the goal. Thus, the characteristics of the real world – that is, PC-2 – are obtained.

At the last, fourth stage, it is necessary to verify the decisions obtained, that is, to compare the characteristics arising from the detailing of the model (PC-2) and the characteristics that actually formulate our goal of activity (PC-1). If these characteristics coincide with those required by the goal, then the information space adequately describes the real world.

To describe complex objects, phenomena, entities and processes, a hierarchically ordered set of information spaces is used, which are interconnected into a single system with the help of certain system-forming principles (which can often be considered as independent ontologies). Fig. Figure 2.2 presents the author's description of the hierarchical structural organization of information spaces [53].

The letters "A", "B", etc., depict subject areas that relate to a certain task (or to a certain scientific discipline). The numbers "1", "2", etc., indicate the levels of the hierarchy.

Fig. 2.3 serves as an example of the hierarchy of meanings (levels) of the description of the essence, because the information spaces of the higher hierarchical level, as a rule, use abstract concepts of a higher level as scientific terms, generalized characteristics, classes, etc. From the methodological point of view, the hierarchy of meanings, which is reflected in the corresponding hierarchy of models, has found its most complete use in physics (see, for example, [67-70]).

In order to form a hierarchical system from individual information spaces, they must have a structure schematically depicted in Fig. 2.3.

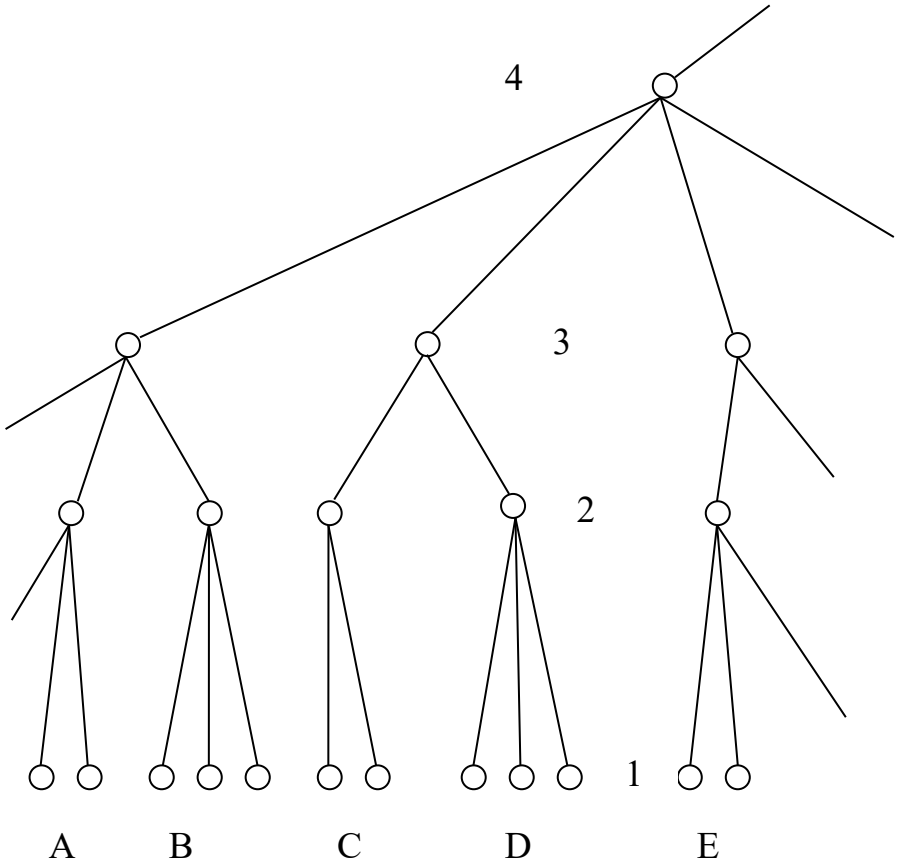

Fig. 2.2. Depiction of the hierarchical organization of information spaces

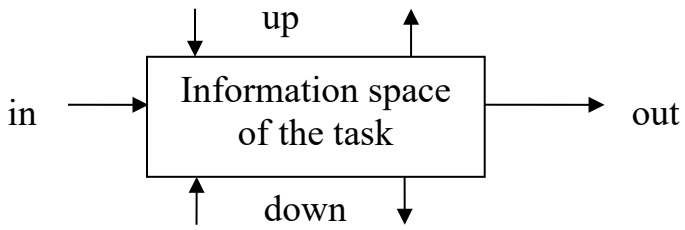

Fig. 2.3. Schematic illustration of the information space as a component of the hierarchical complex

It is reflected here that the characteristics "in" and "out", which are input and output for the information space, respectively, link different information spaces "horizontally", that is, at the same hierarchical level. At the same time, the characteristics "up" and "down" connect this information space with the information spaces of the higher and lower hierarchical levels, respectively.

The hierarchically organized information space of the task is often used to describe the perception of information, decision-making, and the activities of people in a structured social group. In this case, it reflects the characteristic features of the hierarchical ordering of this social group.

2.2 Method of constructing the information space of the subjects of information security

Approaches to building the information space of a person and a social group as subjects of information security. Using the peculiarities of perception and processing of information, decision-making and implementation of activities by a person or a social group, we will analyze approaches to the method of constructing the information space of the task, which describes the activities of these subjects of information security. When presenting this material, we follow the author's publications [43,53,64,65,71,72].

The most effective approach to building the information space, which is dictated by the general methodology of science [40], is as follows:

1) we allocate the subject area (system) under consideration, setting (and fixing) the purpose of activity and methods (technologies) for obtaining quantitative values;

2) we record the states and processes in it, using the methods (technologies) chosen in the previous step to obtain the necessary quantitative characteristics;

3) we carry out "activity", i.e. a planned system of steps, actions (or inaction), etc.;

4) again, after the "act of activity", we record changes in the states and processes of our subject area (system).

In the form of a mathematical model, this algorithm can be represented in the following form.

Let's introduce the following mathematical structures.

G – Multiple Activity Objectives, $g_i \in G$ – a specific target for the activity in question.

SA – the set of characteristics of the subject area within which the activity is carried out, $sa_i \in SA$ – specific characteristics of the subject area within which the activity is carried out.

T – A set of technologies for building an information space, $t_i \subset T$ – a subset of specific technologies that can be used to build an information space for a given subject area and a given activity goal.

In the general case, t_i should be considered as a certain operator that translates the set sa_i and g_i into a specific information space I_i, which describes a given subject area for a given goal of activity. It can be written as follows.

$$I_i = t_i(g_i, sa_i). \tag{2.1}$$

In formula (2.1), I_i is considered as a specific information space for a specific situation, that is, as a set of specific characteristics, parameters, values, etc., which set the subject area of activity at a given point in time.

Using (2.1), the activity of the subject of information security can be represented in the form of the following mathematical relationship.

$$D_i = I_i^{after} - I_i^{before} \tag{2.2}$$

Here, $D_i \in D$ are a description of a specific activity in terms of changing characteristics, parameters, values, etc. D is the space of possible activities, which is set through the information space of the subject area.

In formula (2.2), the dependence of activity on the period of time spent on the activity is explicitly introduced. The activity itself is determined by the difference in the values of parameters, characteristics and values of other variables that are included in the information space of the subject area.

If there are such changes (i.e., $D_i \notin \varnothing$), then there was also an "act of action."

Everywhere in the paper we will consider the activity of subjects (a person or a social group) in a conscious and conscious mode.

In order to proceed to the consideration of the general activities of the subjects of information security, it is necessary to first consider the features characteristic of the act of human activity in general. Essentially, it is an assumption about what a person can (is capable of) performing.

Assumption 1. The subject of information security has the ability to build a certain Picture of the World (or Model of the World), expressed in symbols (parameters and characteristics) that are objective in nature. That is, it has the ability to compress the Real World into a certain ordered system of symbols, which it uses as "terms."

Assumption 2. The subject of information security has the ability to solve problems formulated by him (or other subjects) and expressed in the form of symbols of his own Picture of the World, that is, within the framework of the appropriate information space created by him.

Assumption 3. The subject of information security has the ability to "translate" (transition) between the personal Picture of the World (the information space created by him) and the Real World, and in both directions.

Assumption 4. The subject of information security uses acts of activity as a feedback system, which allows him to adapt (adapt) his own Picture of the World (the information space created by him) to the Real World.

Assumption 5. The subject of information security has the ability to transfer (in whole or in part) his own Picture of the World (the information space created by him) to other subjects of information security: his activities also serve to carry out this process.

It should be noted that the above also sets the direction for teaching the subject of information security how to carry out all of the above "more effectively".

Now, in view of the above, let's define the term "activity of the subject of information security", which corresponds to the ratio (2.2).

Definition 2.1. Activity is the implementation by the subject of information security of such changes in the Real World, which can be described in terms of the Picture of the World (corresponding to the information space of the task) of an individual subject of information security (the same, or another).

The above definition is based on fixing a certain method (method, algorithm, model, etc.) of describing reality, that is, on reducing a real situation to a description in the form of a certain model system – a model Picture of the World, the information space of the task in the subject area for an individual subject. If such a description can be carried out within the framework of a certain set of terms, then we can talk about the possibility of a scientific description of the term "activity". If there is no such possibility, then such a definition will be situational. From this definition it follows that the use of the word "activity" as a scientific term necessarily requires the task of the interior (context) in which this activity takes place, as well as the obligatory task of the characteristics through which this activity is expressed.

Model and method of constructing the information space of the subject of information security (a person or a social group) for the case of using domain databases in the description of an arbitrary system. As can be seen from the ratios (2.1) and (2.2), the task of modeling the subject's activity is reduced to the task of the task of the method of constructing the information space for fixed subject areas and goals of activity. At the same time, it is necessary to use only such variables and characteristics of the subject area that can be used for computer processing, which is described in detail in the author's publications [43,53,63,64,71-76].

It should be emphasized that for the needs of using the characteristics of an object within the framework of information technology, these characteristics, data, parameters, etc., must be presented in a form that allows their further processing on a computer (for example, in mathematical form, in the form of logical or linguistic variables, etc.).

Let's consider a general model with the help of which such a description of the information space can be made. With its use, a complete set of characteristics of the activity of the subject in need of protection is obtained. The information space is defined by such a tuple.

$$K =< DB, G, d_1, d_{1u}, d_{1d}, d_2, NC > \quad (2.3)$$

Here, *DB* is a database of the object on which the activity is carried out;

G – parameters and characteristics that set the purpose of the activity;

d_1 – operator sorting data, characteristics, parameters, etc. (the first dichotomy), as a result of which each characteristic of the object on which the activity is carried out can be attributed to one of the two sets (poles of the dichotomy) or can be recognized as unclassified, i.e. referred to the *NC* set and excluded from further consideration (for example, due to the fact that this characteristic does not relate to the activity, which is given by the objective of activity *G*). The classes of dichotomy are called "generalizing" and "detailing";

d_{1u} – an operator for sorting data, characteristics, parameters, etc. (dichotomy) for the generalizing pole of the dichotomy d_1, which continues to divide the characteristics belonging to this set into two more sets ("boundary" and "structure"), or assign the characteristic in question to the set *NC;*

d_{1d} – a sorting operator for data, characteristics, parameters, etc. (dichotomy) for the detailing pole of the dichotomy d_1, which continues to divide the characteristics belonging to this set into two more sets ("object" and "object relations"), or refer the characteristic in question to the set *NC;*

d_2 – sorting operator of data, characteristics, parameters, etc. (dichotomy), as a result of which each of the previously obtained sets of DB database partitioning is divided into two more sets ("state" and "process") – characteristics that cannot be classified are included in the NC set;

NC – a set consisting of those data, characteristics, parameters, etc., which are not related to the topic of activity *G* or cannot be sorted by the sorting operators d_1, d_{1u}, d_{1d}, d_2.

The use of tuple operators (2.3) leads to the division of the set of characteristics of the subject's activity in the subject area into eight subsets.

The *NC* set includes data, characteristics, parameters, etc., that are not used for activities in accordance with objective *G*.

Let's describe the method of using the tuple (2.3) for specific cases of splitting a *database about a DB* object.

1. Operator action d_1.

First of all, in the description of this particular object, it is possible to distinguish those characteristics that relate to the description of a whole class of objects that are similar to the one under consideration. They characterize not this individual object, but the whole class, and they belong to the whole class of "similar" objects (which is given taking into account a specific activity).

It is also possible to distinguish a set of data that relates specifically to this object. In fact, all of them will be a kind of markers or labels just for him – they will characterize the object under consideration exclusively.

The above can be summarized in the following two definitions.

Definition 2.2. The class of information (data, characteristics, parameters, etc.) that characterizes the object under consideration by describing the class of "similar" objects is called generalizing characteristics or generalizing components of information.

Definition 2.2. The class of information (data, characteristics, parameters, etc.) that characterizes the object under consideration by describing the class of "similar" objects is called generalizing characteristics or generalizing components of information.

2. Operator action d_{1u}.

Within the class of generalizing components of information, a division can be made into two more alternative classes by further consideration of its structure. First, this class contains a description of its "reference elements", which are a kind of "benchmarks for comparison" or "the most typical representatives" of this class. In fact, such supporting elements set the structure of the entire class of possible descriptions of the objects we are considering. Secondly, the class of objects in question must be described using the definition of the limits of its applicability. As a rule, for this purpose, descriptions of those data elements (as well as information, characteristics, etc.), those objects that form a boundary for this class, which separate it from other classes from the same or another classification, are specified.

Thus, within the class of generalizing components of information, it can be further divided into groups according to the following "related" features.

Definition 2.4. A class of information (data, characteristics, parameters, etc.) that are descriptions of "reference elements", a kind of "standards for comparison" or "the most typical representatives" for a given class of objects, and which, thus, set the structure of the entire class of object descriptions under consideration, are called structural components of information. Often, such components of information reflect a kind of "topological" characteristics – that is, they are invariants in comparatively significant transformations of this class.

Definition 2.5. A class of information (data, characteristics, parameters, etc.), with the use of which the boundaries of its application can be described for the class of objects under consideration, which distinguish this class, which separate it from other classes from the same (or other) classification, are called boundary components of information. Often such a separation is a kind of "membrane" ("grid") that "passes" into the class events that have only quite certain characteristics. parameters, data.

3. Operator action d_{1d}.

The class of detailing components of information can also be divided into two more alternative groups. The first group includes data that describe only the concrete object under consideration, regardless of its connections with other objects analogous to it (for example, they describe only this object of activity, only that which distinguishes it, distinguishes it from others). The second group will include only those data that describe the inherent connections of this particular object with other, similar objects.

Thus, we get two more definitions.

Definition 2.6. A class of information **(**data, characteristics, parameters, etc.) about an object that characterizes this particular object and relates exclusively to this object (regardless of its connections with other objects similar to it) is called object components of information.

Definition 2.7. A class of information (data, characteristics, parameters, etc.) about an event that characterizes the description of the inherent connections of this particular object with others (the relations of this object to others, the relationship between this object and others) similar to it (regardless of the description of the object itself) is called the connecting components of information.

4. Operator action d_2.

Finally, the description of the object under study can be divided into two more classes, which are characteristic of each of the four groups of information components listed above. Within each of these groups, information about processes and states can be highlighted. Thus, two more definitions are needed.

Definition 2.8. A class of information (data, characteristics, parameters, etc.) about an object that characterizes the object in question as invariant in time ("frozen", stationary, unchanging, static, "similar to itself") is called static components of information.

Definition 2.9. The class of information (data, characteristics, parameters, etc.) about an object, which characterizes the consideration of the object as variable in time (dynamic, nonstationary, non-invariant in time, "dissimilar to itself"), is called dynamic components of information.

Finally, data about an arbitrary object can be divided into eight non-intersecting classes. In other words, each of the above-mentioned components of data about an object can be attributed to only one of the above classes of information.

Application of the method of constructing the information space of the subject of information security (a person or a social group) for an arbitrary level in a hierarchical system. Following [43,53,64,65,71-81], we will describe the application of the method of constructing the information space in the case when the subject area has a hierarchical structure. At the same time, the result obtained will be universal – that is, suitable for each of the levels of the hierarchy of the subject area. This method is an example of the tuple (2.3).

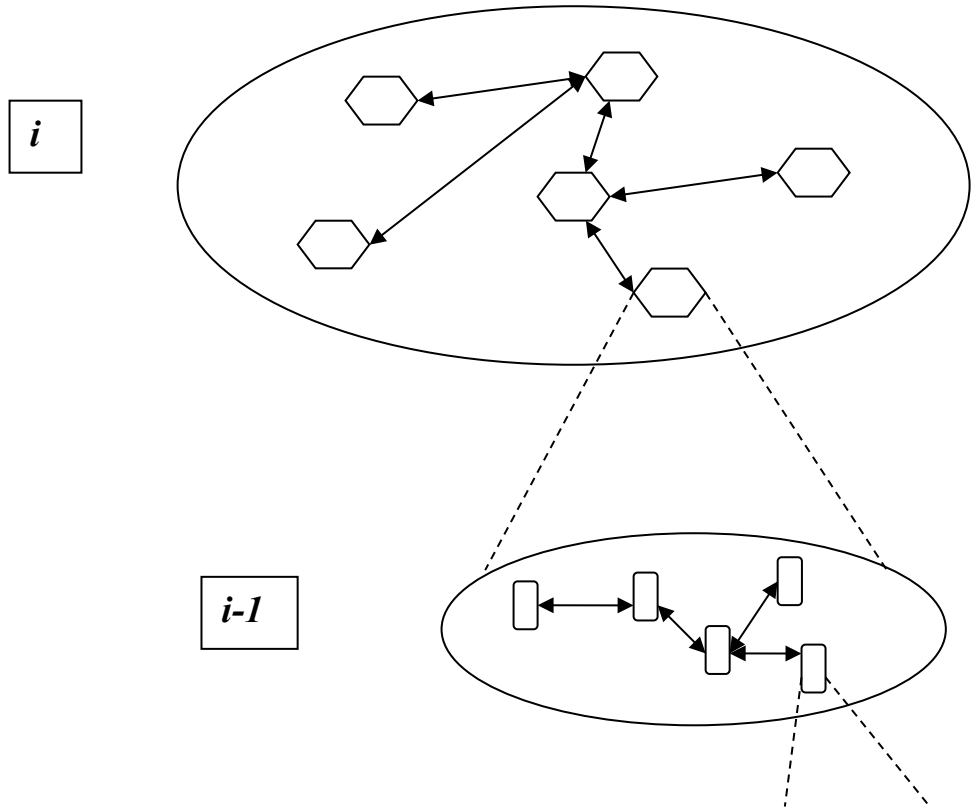

Fig. 2.4. Structural structure of an arbitrary level of hierarchy
for the hierarchical subject area of the subject of information security

The subject area of the subject of information security is built in a hierarchical way, which is shown in Fig. 2.4.

Selection shows that, in some cases, the object from which the level in question is built (denoted in Fig. 2.4 as i) may, in turn, be a hierarchical object of a lower level (denoted as i-1).

Let us describe what data on the structure of an arbitrary level in a hierarchical system are needed to describe its functioning. It is easy to see that when we speak of any one particular hierarchical level, we always mean that such actions must be carried out.

1. Application of the dichotomy d_1, resulting in two sets: one with the characteristics of this hierarchical level as a whole, and the other with the characteristics of the specific elements of this level and the relationships between them.

2. Application of the dichotomy d_{1d}, as a result of which the set of detailing characteristics falls into such two sets.

2a. This level is made up of certain objects that are "the same" in one sense or another.

2b. There is a certain kind of "interaction" between such "identical" objects (in general, both "attraction" and "repulsion"), as a result of which these objects can be combined into a single whole – a single hierarchical level.

3. Application of the dichotomy d_{1u}, as a result of which the set of generalizing characteristics falls into the following two sets.

3a. The hierarchical level as a whole is also considered in its turn as a definite whole, separated, delimited by a certain boundary from the whole environment.

3b. Finally, the entire hierarchical level as a whole has a certain structure, has an internal structure formed as a result of the "interaction" of those objects that make up this level.

This description is universal and can be applied to every hierarchical level.

It is necessary to pay attention to the fact that it is not at all necessary that the single objects that make up some hierarchical level should be completely the same. When applying the method, it is only required that they be "the same" within the framework of the tasks that interest us.

For example, when describing the structure of a company, they are often not interested in the gender of the employees. Of course, for other tasks – for example, statistical – this characteristic of an employee can be important. Or in the case when we prepare a list of functional responsibilities of employees, then we form only a certain list of requirements for them: the list is general enough so that we can have several candidates and so that we have a choice.

In the same sense, the "interaction between objects", the "boundary" and the "structure" of the level are understood.

In particular, the interaction between objects may not be limited to "our" hierarchical level alone. For example, the functional responsibilities of the company's employees (employees of this level of competence) at the initial stage of its emergence do not take into account the so-called "informal" relations in the team. But after a certain period of work, they must be installed. At the same time, the tasks of managing such a team should be subject to review and modification.

Finally, it is important to note that not all objects are included in the level structure.

To describe the functioning of a given hierarchical level in it is necessary to apply another dichotomous division.

4. Let’s apply the dichotomy d_2 to each of the previously obtained four sets. As a result, each of them is divided into two more subsets, which characterize 1) how these objects and properties of the system in question change, and 2) how they, however, retain some kind of "unchanging" state – only then will we be able to describe the level we are considering in its "work".

The first is called the term "process" – adding exactly what it is in. For example: the process(es) in individual single objects that form the hierarchical level in question. A process is information (data, information about characteristics, parameters, etc.), characteristic features that describe the variability of an object. When a process in an object is considered, those of its characteristics that testify to such variability are highlighted.

The second is called "state". For example: the state of interaction between the individual units of this level. A state is information (data, information about characteristics, parameters, etc.) that describes an object as immutable, unchanging, frozen.

Thus, each of the classes of information we have introduced is divided into two more: (1) a description of states and (2) a description of processes.

Thus, there are a total of eight "information components" to describe arbitrary hierarchical systems.

In fact, having set themselves the task of being able to describe the construction and method of functioning of an arbitrary hierarchical system, they came to the same eight basic components of information.

Application of the method of constructing an information space to describe activities in the subject area. Thus, it is shown [43,53,64,65,71,73] that for activities in subject areas (and activities always have a goal), which are described in the form of 1) a database, 2) a certain arbitrary level in a hierarchical structure, and 3) a system, one and the same method of constructing the information space of the problem can be applied, which is represented as a division of characteristics into eight sets that do not intersect with each other.

Schematically, the structure of the subject's information space, consisting of classes-components of information, can be represented by Table 2.1.

Table 2.1. The structure of the components of the subject's information space.

<table>
<tr><td rowspan="8">About
the object</td><td rowspan="4">data on the class
of similar objects
(summarizing
components
of information)</td><td rowspan="2">Class Reference Elements
(Structure, Topology)</td><td>Static,
immutable</td><td>St-S</td></tr>
<tr><td>Dynamism,
variability</td><td>St-D</td></tr>
<tr><td rowspan="2">Boundary between
a given class and others</td><td>Static,
immutable</td><td>B-S</td></tr>
<tr><td>Dynamism,
variability</td><td>B-D</td></tr>
<tr><td rowspan="4">data about this
particular object
(detailing
components
of information)</td><td rowspan="2">The object itself
as singular and unique</td><td>Static,
immutable</td><td>Ob-S</td></tr>
<tr><td>Dynamism,
variability</td><td>Ob-D</td></tr>
<tr><td rowspan="2">Relationships of this object
with other specific ones
similar to it</td><td>Static,
immutable</td><td>L-S</td></tr>
<tr><td>Dynamism,
variability</td><td>L-D</td></tr>
</table>

Thus, a method of constructing the information space, which gives a complete description of the object of activity, has been proposed. At the same time, the definition of the information space itself can be presented as follows.

Definition 2.10. The information space of the task will be a set of attributive parameters and relevant characteristics that allow to describe the entire set of data related to a given goal and subject area of activity with the necessary degree of unambiguousness.

Definition 2.11. The basis of the information space will be called the introduced eight classes of division of the set of characteristics of the task, which will also be called the components of information.

The basic components of the information space will be abbreviated as described in Table. 2.1.

The proposed method allows to form the information space of the task, the components of which meet the following conditions.

$$I_i = \sum_{k=1}^{8} C_i^k \tag{2.4}$$

In this case, for an arbitrary pair of components of the information space k and m, the following condition is fulfilled.

$$C_i^k \cap C_i^m = \varnothing \tag{2.5}$$

Within the framework of the developed method of constructing the information space, the circumstance that, in accordance with the formula (2.2), it will be used only as an intermediate stage in modeling the activities of a person or a social group in the subject area of information and psychological security, is immediately emphasized.

Thus, the developed method of constructing the information space is at the same time universal. The universality of the method lies in the fact that it can be applied to the three most common methods of modeling subject areas – using databases, hierarchical structures and systems, and leads to a single (universal) form of representation of ontology in the form of a set of eight sets of characteristics that do not intersect with each other.

The model of building the information space is based on a number of assumptions.

Assumption 1. The subject of information security operates not with the information space itself, but with the method of its construction.

Assumption 2. The method of constructing the information space depends on:

1) the purpose (goals) of the activity of the subject of information security,

2) the existing database of parameters and characteristics of the subject area of activity.

Assumption 3. The method of constructing the information space is based on the use of attribution of each characteristic:

1) either sequentially to the corresponding pole of each of the 3 dichotomies,

2) or are rejected as irrelevant to the purpose of the activity.

The dissertation shows that these assumptions are fulfilled to build information spaces for:

1) databases of any kind,

2) parameters and characteristics described by systems of arbitrary nature,

3) each of the levels for hierarchical systems and objects of activity of arbitrary nature.

From the methodological point of view, the construction of the model is aimed at its application to forecast the development of subjects and objects. It is the verification of the model on real objects, entities and processes that justifies the assumptions that underlie the model.

The proposed model of formation of the subject's information space allowed to develop and verify:

1) a method of identifying the class of activity for a given person,

2) methods of forecasting the activity of a given person as a class of activity,

3) models of classification of possible relations between classes of activity of given people and methods of forecasting the quantitative level of efficiency of joint activity of two people and quantitative indicators of the effectiveness of information exchange between two people,

4) models and methods of identifying people who are able to carry out effective activities at the highest levels of hierarchical socio-economic structures and systems.

2.3 Formation of a model of integrated protection of subjects of information security in the tasks of information and cybersecurity

Since, according to the definition of the Cisco laboratory, the weakest link in any cybersecurity system is always people, the development of acomprehensive protection of such entities in the tasks of both cybersecurity and information security is extremely relevant.

On the basis of the proposed information space, a methodology for comprehensive protection against the negative information and psychological impact of a person and a social group as subjects of information security is proposed [77], which is presented in Fig. 2.5.

The input data for the formation of the information space of the subject of information security, the formation of a database of characteristics of the results of its activities and the formation of a database of measures to counteract the negative information and psychological impact on it are the tuple:

$$K^{Si} =< BD^{Si}, G^{Si}, C^{Si}, AS^{Si} >, \quad (2.6)$$

consisting of the set G^{Si}, which sets the purpose of the activity of the subject of information security, set C^{Si}, which specifies a constraint on the subject's activity, set AS^{Si}, which defines the subject area of activity and database BD^{Si}, which describes the characteristics of the activity of the subject of information security. The Si index denotes the subject of information security: an individual subject CS, an non-structured social group (NSG) – NSG, Structured Social Group (SSG) – SSG, organized social environment (OSE), to which the subject adapts – OSE, one-level social network (OSN) – OSN, multi-level social network (MSN) – MSN.

The result of the methodology is the identification of measures to counteract the negative information and psychological impact on the relevant subject of information security. Its implementation consists in the implementation of five stages.

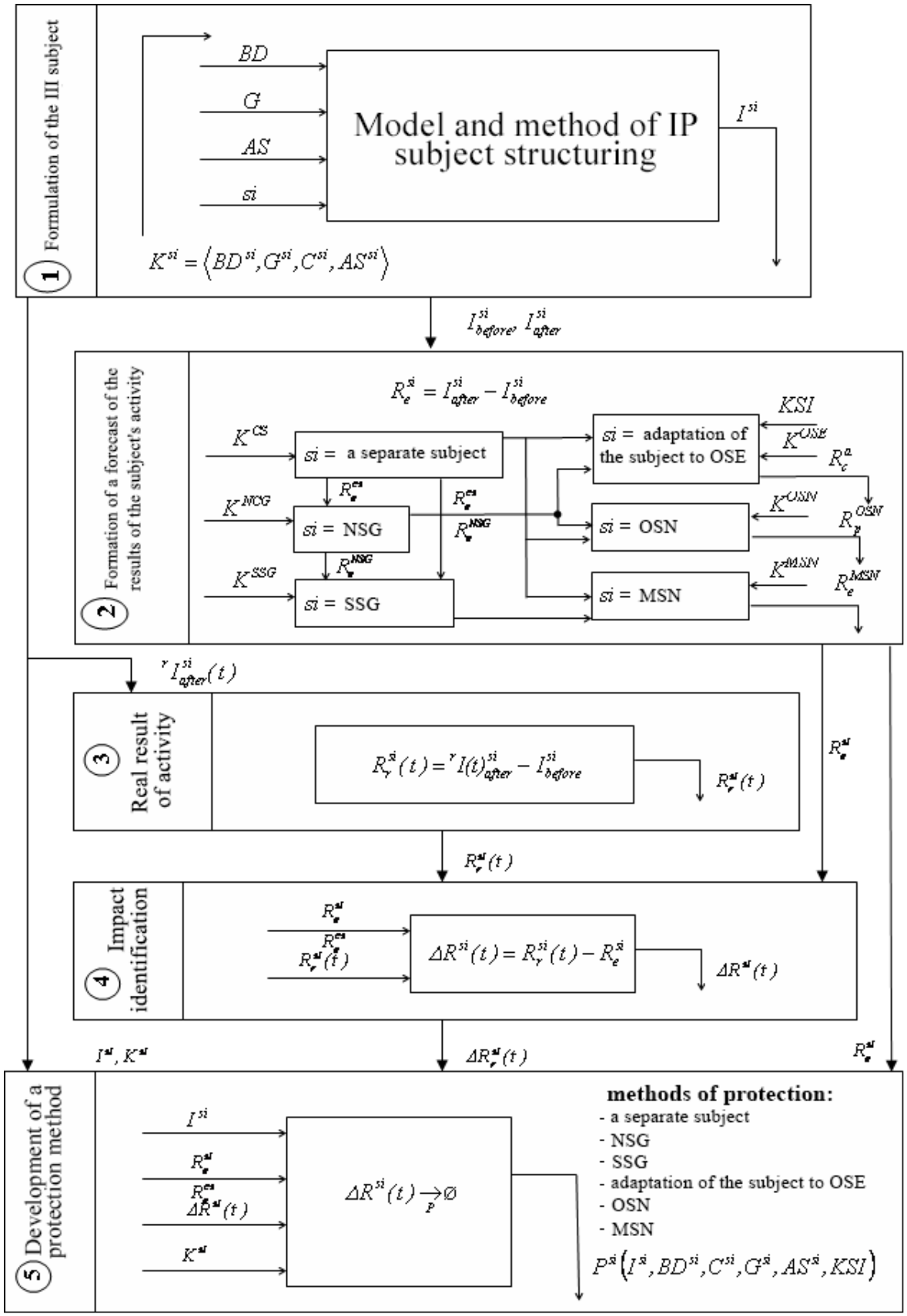

Fig. 2.5. Methodology of comprehensive protection against negative information and psychological influence of a person and a social group as subjects of information security

Stage 1 – structuring the information space of the subject of information security. The implementation of the stage consists in the application of the developed model and method of structuring the information space of the subject, which requires protection from information and psychological influence, which takes into account the target components of the set that determines the activity of the subject in the subject area, as well as a step-by-step dichotomous division of the full set of characteristics of the subject's activity into eight subsets (the dichotomous poles "state – process", "generalized – detailing", etc. are taken into account). The input information is the tuple (2.6), and the output information is the information spaces (PI) to I_{before}^{Si} and after I_{after}^{Si} carrying out activities by the relevant subject of information security.

Stage 2 – a theoretical (exemplary) database of the results of the activities of the relevant subject of information security is formed.

The theoretical database of performance results is determined by the following formula

$$R_e^{Si} = I_{after}^{Si} - I_{before}^{Si}. \qquad (2.7)$$

In (2.7), the *value of I* after is taken from stage 1 as a theoretical (forecast) value of IP, which is obtained after the implementation of a given activity by the relevant subject of information security Si.

Depending on the choice of the subject Si, resultant database R_e^{Si} is formed as follows.

For $Si = CS$ the inputs are K^{CS}, and the outputs – R_e^{CS}.

For $Si = NSG$ the inputs are K^{NSG} and R_e^{CS}, and the outputs – R_e^{NSG}.

For $Si = SSG$ the inputs are K^{SSG}, R_e^{CS} and R_e^{NSG}, and the outputs – R_e^{SSG}.

For $Si = OSE$ the inputs are KSI, K^{OSE}, R_e^{CS}, and R_e^{NSG},

and the outputs – R_e^{OSE}.

For $Si = OSN$ the input is the code of the social institution for the DSO K^{OSN}, R_e^{CS} and R_e^{NSG}, and the outputs – R_e^{OSN}.

For $Si = MSN$ the inputs are K^{MSN}, R_e^{CS} and R_e^{SSG}, and the outputs – R_e^{MSN}.

Thus, the theoretical (forecast) databases of the results of the activities of some other subjects are included for the majority of subjects. This stage is given in detail in the following sections of the dissertation.

Stage 3 – a database of real (actual) results of the activities of a certain entity at a given time is formed. At this stage, the database of real results of activities carried out by the relevant subject of information security is determined by the formula (2.8)

$$R_r^{Si}(t) = {}^{r}I_{after}^{Si}(t) - I_{before}^{Si}. \quad (2.8)$$

The input characteristics are the type of subject of information security Si, information space ${}^{r}I_{after}^{Si}$ of this subject, which is currently formed from the database of real characteristics after the implementation of its activities, and the IP of this subject I_{before}^{Si}, which was built before the start of the activity.

For the case of NSG, the method is detailed later in the dissertation.

Stage 4 – a database of differences between the real results of a certain subject and the forecast results at a given point in time is formed. This database (the initial characteristics of the stage) is determined by the formula (2.9)

$$\Delta R^{Si}(t) = R_r^{Si}(t) - R_e^{Si}. \quad (2.9)$$

The input characteristics of the stage are the output characteristics of stages 3 and 2, that is, respectively, the database of characteristics of the real results $R_r^{Si}(t)$ of the subject's activities and a database of theoretical characteristics R_e^{Si} of the subject's activities.

Stage 5 – development of measures to counteract the information and psychological impact on the identified subject of information security. The initial characteristics are a database of countermeasures $P^{Si}(I^{Si}, BD^{Si}, C^{Si}, G^{Si}, AS^{Si}, KSI)$, which depends on the subject's information space I^{Si}, databases of the subject's activities BD^{Si}, restrictions on the activities of the subject C^{Si}, Objectives of the subject's activities G^{Si}, subject area of the subject's activity AS^{Si} and, if necessary, from the OSE class KSI. This database is based on the optimization problem

$$\Delta R^{Si}(t) \xrightarrow[P]{} \varnothing . \qquad (2.10)$$

The input characteristics are the input characteristics of the previous stages.

Thus, the monograph develops a methodology for comprehensive protection of a person and structured and unstructured social groups, taking into account the possibility of adaptation of individual subjects in need of protection and their groups to the organized social environment, as well as one- and multi-level social networks from negative information and psychological influence, which takes into account the classes of characteristics of the activity of an individual subject and a finite set of classes of binary relations between these subjects with the use of certain operators, which made it possible to ensure the protection of various kinds of subjects and subject groups from negative information and psychological influence.

The proposed methodology of comprehensive protection of a person and social groups as subjects of information security from negative information and psychological influence is applied to an individual subject, to social groups (structured and unstructured), to subjects that adapt to the organized social environment and to one- and multi-level social networks. The proposed methodology can be used as a basis for the development of a wide range of methods and means for the protection of subjects information security from negative information and psychological influence, which allows it to be used to develop powerful cybersecurity tools.

Formulating a model of comprehensive protection of information security subjects in the tasks of information and cybersecurity, it is necessary to highlight the use of human imitator bots (HIB) as a particular danger. The development of artificial intelligence systems leads to the fact that HIBs are getting closer and closer to satisfying the Turig test. These bots work in a dialog mode, and even today their identification requires quite a lot of effort from the person with whom the HIB communicates.

This allows the HIB to be programmed in such a way that it carries out the *motivation* of human communicators to take certain actions.

Recent events in South Africa and other countries have shown that social networks are the *referential* medium that can unite people around certain ideas (ideologies) and encourage them to work together in *physical* (real) space. If we take into account that aspects of ideology are quite easy to single out and algorithmize, and for *ideological interpretation of* real situations it is quite easy to build an appropriate ontology, then the use ofHIB is becoming an important element of information security today.

This problem is highlighted in many publications of domestic and foreign authors, among which V. Akman, V.M. Bogush, V.L. Buriachko, G. A. Manoilo, A. Saigin, A. Turing, M. Halms, V.O. Khoroshko, I. Tsitsekly and others should be highlighted.

However, most scientific works are focused on the problem of *creating* such artificial intelligence that *the* Turing test can satisfy [1-4].

The problems of information security that arise in connection with these works, as a rule, are the subject of literature and cinematography only.

The Turing test refers to identifying the capabilities of information technology and artificial intelligence as a "substitute" for human intelligence. It was first published in 1950 [1].

Essentially, Turing's problem is: "Is there a mind other than the mind of Man?" This task had a pronounced applied character, which manifested itself already in the late 1950s.

Man went into space. And this led to the fact that she could meet with alien *intelligence*, with alien *intelligent beings*. And on the agenda was the need to develop

a kind of "test for reasonableness". This is necessary both in order to let *others* pass through it. But the main thing is that *we*, Humanity, will need to pass this test.

Without going into the history of the question, the different wording of the test itself and the results obtained [2-4]), note that there is still no correct solution.

Purpose. The main purpose of the article is to develop a method to protect a person from negative information and psychological influence through BILs by identifying and isolating them.

Statement of the main material. In [5,6] it is proved that there are universal algorithms for constructing ontologies loaded with a goal (structuring the information space of the problem) and that the implementation of activities to solve it can be classified. Two fundamentally different modes of activity were also distinguished.

The first mode *D1* is an activity that is performed by the subject, provided that the subject acts in accordance with "internal" factors: he himself chooses one goal from a set of possible goals, and specific methods and technologies (from the corresponding set) to achieve it.

The second mode of activity *D2* is the activity of the subject, which is conditioned by factors "external" to him. This regime is called "normative". In fact, it corresponds to the activity according to a well-defined algorithm.

In [5,6] it is also proved that voluntary activity performed by a person can be attributed only and only to one of the above two modes of activity *D1* or *D2*.

The problems of identifying the mode *of activity D1* and the mode of activity *D2* have fundamentally different complexity.

If the identification of the mode of activity *D2* can be reduced to the problem of identifying one algorithm from a given limited set of algorithms, then the problem of identifying the mode *D1* can be reduced only to the problem of identifying a certain class of algorithms from a given set of classes.

Thus, the Turing test can be reduced to the task of identifying the mode of activity D1 or the mode of activity D2 in the process of communication. At the same time, the identification of mode *D2* is uninformative: this mode of activity is inherent in both a person and a technical object.

If, on the other hand, in the process of communication, the mode of activity *D1* is identified, which belongs to only one and only one type, then the Turing test will be completed. Indeed, man belongs to one and only one particular class of activity algorithms, which is invariable throughout a person's life.

For a HIB that is able to pass the Turing test, the results obtained require the corresponding algorithm to comply with certain requirements.

1) HIB should include a database/knowledge base on a certain class of tasks "for activity" within at least one given interior of activity (its choice should correspond to the characteristic aspects of human activity).

2) HIB should include examples of methods and technologies for solving the relevant classes of tasks "for activity".

3) HIB should include "history", which is a time-ordered set of interiors of activities and methods and technologies for carrying out activities within their framework.

4) HIB should contain a database/knowledge base on "normative" methods and technologies of activity in "standard" interiors.

It should be emphasized that the absence of at least one of these requirements makes it possible to accurately identify IT in the communication process (of course, provided that IT "plays the role" of an adult).

Thus, the limitations imposed on the "Turing test" by the presence of a person's type of activity according to [5,6] are formulated, which is, in fact, a method for developing systems of protection against negative information and psychological influence from the HIB.

It should be emphasized that the absence of at least one of these requirements makes it possible to accurately identify the HIB in the process of communication (of course, provided that the HIB "plays the role" of an adult).

Informing a person that certain ideas and ideologies have been formed as a result of communication with *artificial* intelligence is in itself a very effective means of counteraction: most people today will have a negative psychological attitude from the fact that they have "followed the lead of the computer".

Research results. Fig. 2.6 shows the structure of the algorithm for the functioning of the HIB, which is able to pass the Turing test. From the structure of Fig. 2.8 shows that the directions of HIB identification can be as follows

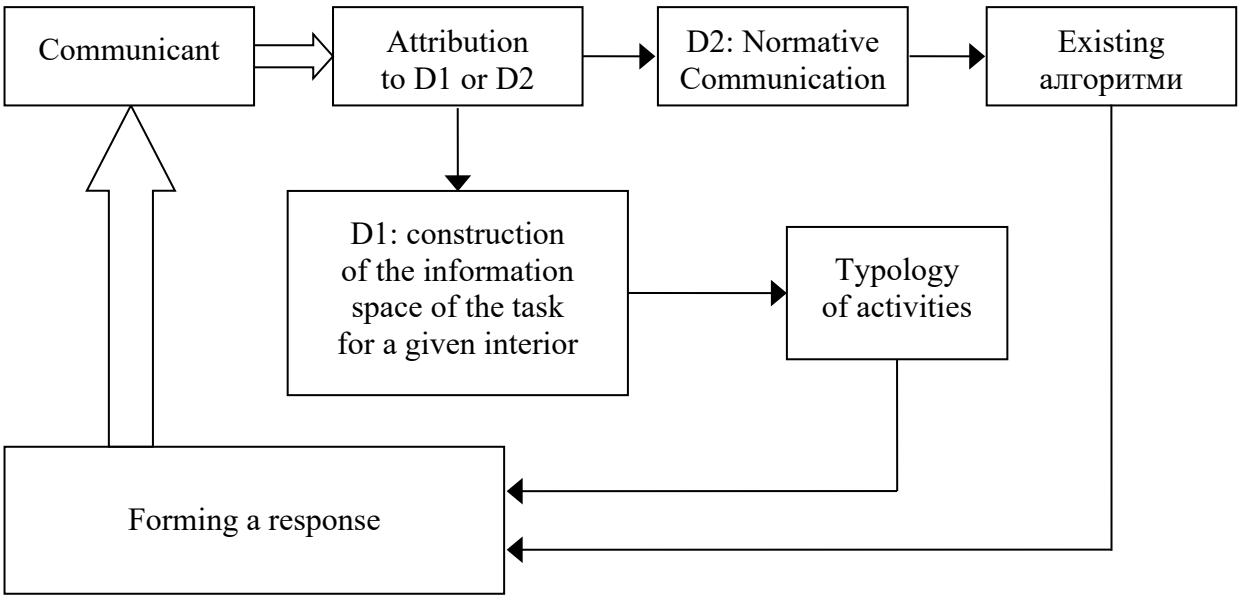

Fig. 2.6 Block diagram of the algorithm for communication

1. Upon receiving a message from a communicator, the HIB passes it through a filter that assigns the message to either the normative mode of communication *D2* or the typical mode of communication *D1*. This filter works according to a specific program, and therefore, using various forms of communication, the essence of which remains unchanged, and taking into account the specifics of the Ukrainian language (which belongs to the *inflectional* languages), it is possible to detect the presence of a filter for "failures" that will manifest through HIB responses.

2. For the normative *D2* communication block, the identification of the HIB is carried out by the correspondence of its messages to the subject area (ontology) in which the HIB has declared its competence. For example, it is quite easy to find compliance with the revealed competence within the framework of a certain professional activity.

3. For the typical communication unit *D1*, the presence of "failures" in the functioning of the HIB is manifested in the fact that it will give examples of such decisions that are not inherent in its type (or which are inherent in *another* type) in messages about rational decisions made by it.

4. Also, for typical *D1* communication, it becomes possible to detect HIB "failures" by the reasoning it uses.

It should be noted that "failures" in the functioning of HIB can be understood as the avoidance of communication on certain topics, on certain sentences formulated in a certain way, etc.

2.4. Conclusion to Chapter 2

1. The paper is the first to develop a model for constructing an information space for a given subject of information security, which is based on the specifics of perception and processing of information, features of decision-making and implementation of activities of the subject of information security, which led to the division of an integral database into eight subsets using three dichotomous operators.

2. The paper describes the method of using the information space of the subject of information security to protect subjects from attacks on the components of the information space, to identify the presence of such influence and its specific characteristics, as well as to counteract the negative information and psychological impact on the formation of an adequate goal of the information space.

3. For the first time, a methodology for comprehensive protection of a person and structured and unstructured social groups has been developed, taking into account the possibility of adaptation of individual subjects in need of protection and their groups to the organized social environment, as well as one- and multi-level social networks from negative information and psychological influence, which takes into account the classes of characteristics of the activity of an individual subject and a finite set of classes of binary relations between these subjects using certain operators, which made it possible to ensure the protection of various kinds of subjects and subject groups from negative information and psychological influence.

4. The development of the theory of artificial intelligence makes it possible to create human imitation bots that will be difficult to identify. They can be used to exert a negative informational and psychological impact on a person by influencing his ideas and ideology. This, as a result, can affect a person's activities in the real world. The article develops a method of protecting a person from such influence. The method is based on the ways of identifying the communicator as a bot imitating a person: after that, in order to protect a person from its influence, it is enough to inform him that he or she has communicated with a "robot".

CHAPTER 3 ENSURING INFORMATION SECURITY AND CYBERSECURITY: MODELS, METHODS AND TECHNOLOGIES OF PROTECTION

3.1. Generalized model ofactivity of subjects of information security in the information space

We will apply the concept of information space to build a model of activity of the subjects of information security in the information space of the task, and then, using it, for the model and method of protecting the subject of information security from negative information and psychological influence. To build a model of activity of the subject of information security, we will introduce the following definitions.

Definition 3.1. A set of characteristics of the elements of the subject area, which are attributed to a certain component of the information space of the subject of information security, is called the filling of this component of the information space, taking into account the purpose of the activity.

Definition 3.2. Activity within a given subject area consists in changing the content of the components of the information space, which is built according to the universal method.

In the future, we will use the terms "information space of the subject of information protection, taking into account the purpose of the activity" and "information space" as synonyms.

The article proceeds to the description of the method of linking information spaces "before" the management and/or activities of the subject of information security and "after" the implementation of this. That is, the information space that the subject builds before the implementation of management ("action"), and which, in fact, programs it for activity, and the information space that the same subject builds – within the framework of the same task – to make a decision on whether the effect of the management carried out by him has been achieved.

Definition 3.3. The transformation (change) of the content of the components of information will be called activity or management.

This definition is algorithmic because it explicitly defines a procedure for determining the presence of management. In particular, it makes it possible to get an

answer to the question of whether an act of management was carried out in the system under consideration. To do this, it is necessary to carry out three successive stages.

1. It is necessary to distinguish eight characteristics of the object of management – eight components of information, dividing the database into eight classes, which describe the degree of fullness of the components of information for our system. Thus, we get a description of the system at a certain point in time.

2. Do the same procedure some time later.

3. It is necessary to compare the descriptions of the studied system "before" and "after", that is, at the initial and final moment of time.

If the characteristics of the system have not changed within each of the basic components of information, then the implementation of activities (management) over the object/system has not been carried out. If such a change is observed, then the very fact of the influence is recorded.

Definition 3.4. An object that perceives (assimilates) the content of the components of information in the system under consideration, and which is capable of transforming (changing, transforming) the content of the components of information in it (at the same and/or another hierarchical level) is called an abstract information automaton (AIA).

In the above definition, the ability of AIA to change the content of information components, for example, to change states and/or processes in the system, is clearly highlighted. In fact, AIA is considered as a separate independent object (a certain separate system), which is capable, in response to the influence of external conditions, to accordingly change some characteristics of the objects of activity (for example, production or organizational structures).

AIA can be considered as an object that has the following structural structure:

$$<input \mid output>. \tag{3.1}$$

Or

$$<Perception\ Block \,/ \text{Activity.} > \tag{3.2}$$

Designed in this way, AIAs perceive certain components of information as their first block and transform them into components of information, within the

framework of which the activity of this AIA takes place. In other words, AIA, which is built in accordance with such a rule, can be considered as an object that implements a set of methods (algorithms, modes, methods, technologies, etc.) to carry out activities in the system.

We will build a mathematical apparatus to describe the activities of AIA in the information space.

According to (3.1) or (3.2), the AIA driven above can be considered as an operator in the information space, more precisely in the space of the information component.

To do this, using the above basis of the components of information in the information space, we write down arbitrary information about the system in the following form (see, for example, [85]).

$$I = \sum_{k=1}^{8} I_k \cdot \vec{i}_k \tag{3.3}$$

Here i_k are the basis vectors of the information component space, which define the names of the information components (they are listed in Section 2). I_k are characteristics that can be attributed to a given component of information (i.e., the content of these components of information).

The relation (3.3) is understood in the sense that I_k represents a certain database that refers to a certain given class of information – a given component of information. For example, if i 1 denotes the information component *St-C*, then i_1 denotes the entire set of parameters and characteristics (the entire database) that describes this particular component of information for the problem we are considering. In this sense A "point" in the information space is a set of databases that do not intersect with each other, and each of which refers to only one component of information.

Note that I_k is not a number, as a result of which the operation of "component-by-component addition" should be defined as the union of two homogeneous (i.e., those that describe the same component of information) bases into one. "Component-by-component subtraction" is defined similarly. In some cases, the information space may well be equipped with an appropriate metric (for example, similarly [86,87]).

Thus, the activity of AIA in the information space can be represented in the form of the operator *G*, which converts the *information I* before about a given object over which the activity is carried out (for example, a production or organizational structure), which was before the implementation of the management act, into the *I* after information about the same object, but which takes place *after* the implementation of the management act. This can be written as follows:

$$I_{after} = G \cdot I_{before}. \tag{3.4}$$

It is easy to see that the operator G defined in this way has the following property: if the information space of the problem is divided into two subspaces I b1 and I b2, then G(I b1 + I b2) = G(I $_{b1}$) + *G(I $_{b2}$)*. This property is a consequence of the fact that the solution of a set of problems, each of which is obtained by decomposing the main (complex) problem into complementary parts, each of which is solved separately, is equivalent to solving the initial complex problem. Of course, this is done in the case where synergy and nonlinearity effects are absent [53,71]. But this, in fact, means that the subspaces I$_{b1}$ and I_{b2} of the information space do not intersect (that is, they do not have common points).

Thus, *the information space* I_{before} is broken down into a direct sum of subspaces [85-88].

$$I_b = \sum_k \oplus I_b^k, \quad \forall k, m : I_k \cap I_m = 0 \tag{3.5}$$

As a result, *the G* operator acts as follows:

$$I_a = \sum_k \oplus I_a^k = G\left(\sum_k \oplus I_b^k\right) = \sum_k \oplus G\left(I_b^k\right). \tag{3.6}$$

In general, it follows from (3.6) that the *operator* G can be represented as a tensor operator that has n "lower" and *m* "superscripts". At the same time, due to the presence of a basis in the information space, the number of both "upper" and "lower" components of the tensor $G(n)^{(m)}$ is limited to 8: $n,m8.\leq$

For the sake of simplicity of notation, let us stipulate that the "lower" components correspond to the components of information for the *information* space I $_{before}$, and the "upper" components correspond to I_{after}, respectively.

Using properties (3.5) and (3.6), we conclude that the action of any tensor operator G(n)(m) is expressed in terms of the action of the sum of $max\{m,n\}$ quasilinear operators of the form $g^{and}{}_{k}$.

This statement can be formulated in the form of the following theorem.

Theorem 3.1. To carry out any activity, it is necessary and sufficient to have only such AIAs that are programmed by one component of information (from the information space I before) and whose activity is also expressed in the change of one component of information from the *information* space I after (i.e., the resulting change in the transition from I $_{before}$ to I $_{after}$ is a change in the information space I_{after} only one component compared to the I_{before} information space).

Proof. The validity of this theorem is based on the fact that the information space is a database of characteristics, parameters, etc., that relate to the problem we are considering.

In this sense, any operator AIA: I $_{before}$ $I \rightarrow_{after}$ acts as an automorphism, that is, in fact, it does not change our information space: only the "fullness" of its coordinates, i.e. the numerical (or other) values of its components, changes. For other "two-component" AIAs, the result of the "previous" AIA is a programmable information space. The chain can be continued as long as necessary.

That is, there is an equality (in the sense of filling the components of the information space) I $_{before} \rightarrow I_{after} = I_{before} \rightarrow I^{1}_{after} \rightarrow I^{2}_{after} \rightarrow ... \rightarrow I_{after}$, where the "intermediate" information spaces differ only in one component of information.

The sufficiency of the theorem stems from the fact that, comparing only the "initial" information space and the "finite" information space with each other, we will not be able to determine whether the control was carried out by the operator $G(_{n})^{(m)}$ or whether it was carried out by a set of successively applied "two-component" operators $g^{and}{}_{k}$.

In other words, we can "replace" a single activity (management), which is based on a set of components from the information space, with the sum of successively applied acts of activity, each of which "uses" only one component from the information space I $_{before}$ and the result of which is expressed in the change of only one component of the information space I $_{After}$ This statement is a standard method of "breaking down" a complex task into sequential stages. As a rule, quite often such a breakdown into successive stages is carried out by the subject of information security "without even thinking", that is, as "obvious".

Thus, by virtue of Theorem 3.1, each operator corresponding to AIA can be expressed as the sum of certain "binary" linear operators that link together only two components of information: one from the I_{before} space and the other from the I_{after} space. Mathematically, it can be written as follows.

$$g_{(n)}^{(m)} = \sum_{k=1}^{\max(n,m)} g_{(k)_i}^{\ j} . \qquad (3.7)$$

It is easy to see that the following statements will be true for *the introduced operators* g^i_k.

Statement 3.1. The operator g i k is commutative g i $_k$+g n m=g $_n$ ^{m}+ g ^i_k and associative g1+(g $_2$+g $_3$)=(g $_1$+g $_2$)+g$_3$.

The proof follows from the properties of the operators g^i_k.

Statement 3.1. The total number of g^{and}_k operators is 64 different variants.

Proof. The binary operator g^i_k can have only one of the eight components from the I_{before} information space and only one of the eight components from the I_{after} information space. The number of different possible options is 8×8=64.

Here are some examples of how the *operators* g^{and}_k can be used to describe control. The general method of creating automated process control systems on the basis of abstract information automata is given in [89].

Example 3.1. Consider a centrifugal regulator, an example of which is the Watt regulator [90]. From the point of view of the AIA introduced above, it is a management that is arranged according to the following algorithm.

$$<process \mid state> \qquad (3.8)$$

Of course, this considers a very specific characteristic of the object to be managed.

The regulator monitors a certain characteristic of the object, and then carries out its activities in such a way as to achieve its immutability – that is, to achieve a certain state (specified for this characteristic).

Example 3.2. Another example is a regulator that does not allow, for example, flutter (a set of self-excited non-damped torsional and bending vibrations of aircraft

structures that lead to its destruction) [90]. In this case, the AIA, which carries out its activities, is arranged "in reverse".

$$<process \mid state> \tag{3.9}$$

For this purpose, the AIA also considers a very specific characteristic of the object to be managed.

The regulator (2.10) monitors a set of values (i.e., states) of certain characteristics of the object being controlled. And its activity consists in initiating processes that are aimed at changing the "critical" values of the same characteristics for the object.

Interestingly, a similar algorithm (3.9) can also be used to describe a whole class of regulators that aim to prevent parametric resonance of structural elements of an object (for example, those that correspond to the so-called "Arnold languages" [91]).

It is also possible to give examples of AIA, which have long been widely used as standard elements in the theory of control of both artificial and natural objects. Fig. Figure 3.1 shows a block diagram of a parallel feedback model, which is widely used in technology for control systems [90].

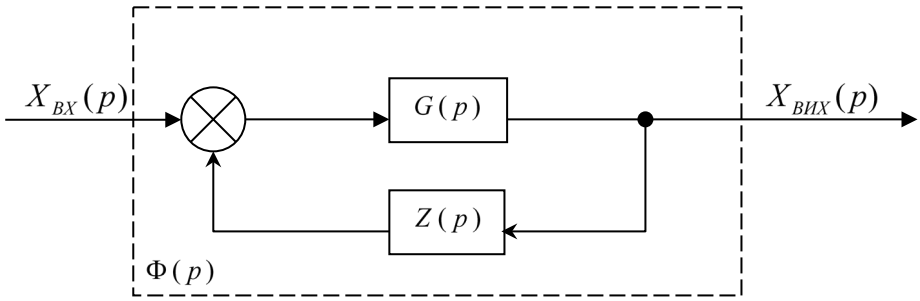

Fig. 3.1. Block diagram of the parallel feedback model

Example 3.3. In general, negative feedback is given by the expression (3.8) [90,92-95]. But, unlike the previous examples, it can already use several components of the information space of the task.

Example 3.4. A positive relationship is given by the expression (3.8), where, in the general case, several components of the information space of the problem can also be used [90,92].

As can be seen from Examples 3 and 4, a large number of standard problems of the general theory of automatic control and cybernetics in general allow the use of the AIA concept as standardized elements.

But the subject area of AIA is much wider than control theory and cybernetics. Let's give an example when AIA can be used as an analogue of "natural language" to build intelligent systems in information technology.

Example 3.5. Let's consider the problem of automatic rating formation when the number of rating elements is less than the number of rated objects. At the same time, only those objects that exceed certain specified conditions need to be rated. Moreover, if the task is given, such a rating must be constantly changed, taking into account the current changes in the characteristics of the rating objects.

For this task, AIA is suitable, which has the following structure. It is this element that selects the required number of rated objects.

$$<Гр\text{-}П \mid Гр\text{-}С> \tag{3.10}$$

Indeed, under the condition of the task, it is necessary to take into account the process of changing the characteristics of objects, constantly comparing their current values with the specified ones. The rating itself is an object that is the result of activity.

The components of "input" and "output" information belong to different information spaces. In the course of further exposition in our book, we will not, as a rule, emphasize this circumstance in particular.

In functional form, such an operator describing control at one specific (given) level in a hierarchical system can be written as

$$<entrance \mid exit>. \tag{3.11}$$

That is, in the form characteristic of the description of a cybernetic "black box", at the input and output of which there is only one component of information. This "black box" is a certain object that is capable of exercising control in a hierarchical system, and which we will henceforth call an abstract information automaton (AIA). This object, according to our definition, is capable of perceiving

only one component of information about this hierarchical level in a hierarchical self-organizing system, and the result of its activity at this hierarchical level can also be described within the framework of only one component of information.

Let's consider the simplest set of AIAs – two-component AIAs, or, for short, 2AIAs. Let's define them as follows (the names of the basic components of information are given in Chapter 2).

Definition 3.5. An AIA is said to be two-component (2AIA) if it satisfies the following conditions:

1. Each AIA perceives only one component of information and carries out activities within the framework of only one component of information.

2. For each AIA, one component describes static, while the other describes dynamism.

3. For each AIA, one component is generalizing, and the other is detailing.

The correct definition of 2AIA as an object that implements certain methods (types, methods, algorithms, modes, ways, etc.) of activity/management is possible only as described above.

Indeed, the first condition is that 2AIA operates with only two components of information.

Now let's assume that we have defined 2AIA in such a way that some of them implement control (i.e., both program and create) only by detailing components, while others only by generalizing ones. In this case, it will be necessary to introduce a special new type of 2AIA, which would "analyze" the situation at the entire hierarchical level, and would distribute tasks for "detailing types of 2AIA". Thus, the third condition also follows from the requirement of optimality for management implemented by the 2AIA system ("Occam's razor": there is no need to multiply entities unnecessarily).

And if we assume, for example, that 2AIA is both programmed by a process and also creates a process, then we also do not get optimal control. In fact, the principle of "Occam's razor" will also apply here: you will still have to introduce such 2AIAs that have the form *of* <*state*|*process*> – as well as <*process*|*state*>, because only such "new" 2AIAs can organize "communication" in the environment of such 2AIAs. For example, this is necessary in order to "set tasks" for such AIAs. Therefore, the second condition is also necessary.

Note also that with any other definition of 2AIA, their number will be greater: therefore, the class of 2AIA we have introduced is in this sense the "minimum necessary".

To carry out activities (management) in hierarchical structures, 2AIAs are arranged in such a way that one of their components (we will also use the name "function" for it) corresponds to the considered level of the hierarchy as a whole, and the second of its components corresponds to specific individual objects from which this level is built. Schematically, this is shown in Fig. 3.3, where the summarizing and detailing components of the information are denoted through Gen (generalization) and Det (detailing), respectively. From Fig. Figure 3.2 shows that class 2AIA creates feedback rings. As we have seen above, to do this, we need to define the G operator we have introduced as 2AIA.

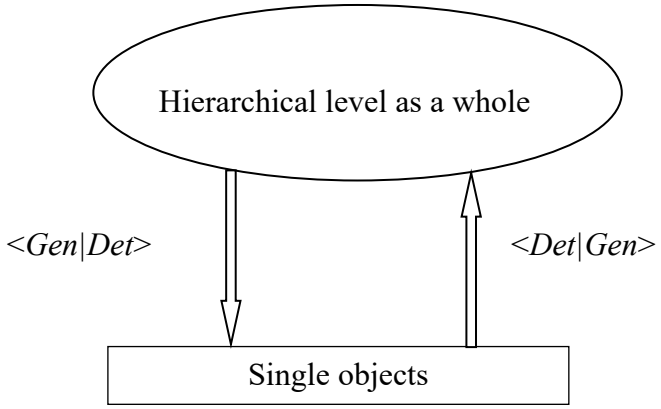

Fig. 3.2. 2AIA as objects that transform the components of information in the information space

The number of different classes of 2AIA can be counted as follows. First, any component of information can be chosen as an "input" component. So, there are eight different possibilities. But as the second component of information, it is necessary to discard a number of choices for the components of information. First, one must discard all those components that describe the same temporal dynamics, i.e., the four components of information (e.g., if the input component is static, then the output component of information cannot be static). Next, the components of information that describe the same hierarchical level as for the input component of

information should be discarded (for example, if the input component of the information is generalizing, then the output component of the information cannot be generalizing). There are no more restrictions in the definition of 2AIA. As a result, there are 2 components of information that we can take as an output – provided that the input component of information is specified. For example, if the input component of information is generalizing and dynamic, then any of the two components can be taken as the output: static and detailing (i.e. *Об-С* or *Зв-С*).

Thus, we come to the following statement.

Statement 3.3. Arbitrary activity in general can be carried out by a combination of 16 classes of 2AIA, which are as follows:

<Ст-С|Зв-Д>, <Ст-С|Об-Д>, <Ст-Д|Зв-С>, <Ст-Д|Об-С>,

<Гр-С|Зв-Д>, <Гр-С|Об-Д>, <Гр-Д|Зв-С>, <Гр-Д|Об-С>,

<Об-С|Ст-Д>, <Об-С|Гр-Д>, <Об-Д|Ст-С>, <Об-Д|Гр-С>,

<Зв-С|Ст-Д>, <Зв-С|Гр-Д>, <Зв-Д|Ст-С>, <Зв-Д|Гр-С>.

The first component of information corresponds to the entrance to 2AIA, i.e. the description of the component of information by which this 2AIA is programmed to act (i.e., which it perceives) and the second component describes the component of information within which its activity can be expressed. Recall that these components of information are taken at different points in time.

Conditions of the theorem 3.1 and statement 3.3 leads to such a statement.

Statement 3.4. To carry out arbitrary activities in an arbitrary information space, it is necessary and sufficient to have 16 classes of 2AIA. In other words, in order to implement an arbitrarily complex and sophisticated activity/management, it is necessary and sufficient to have only such 16 classes of 2AIA as defined above. In fact, a classification of all possible types of management has been built. Statement 3.4 says that there simply cannot be "other classes of 2AIA".

Let us show that 2AIA, from the point of view of control theory and cybernetics, are deterministic finite automata [96].

Modeling the activity of a management agent as a deterministic finite automaton is quite attractive due to its functionality, since a deterministic finite automaton is a special type of abstraction used to describe the path of change in the state of an object depending on the achieved state and information received from the outside. A deterministic finite automaton (DFA) is defined by the following tuple [97].

$$A = \{Q, \Sigma, \delta, q_0, F\}, \tag{3.12}$$

where A – the name of the deterministic finite automaton,

Q – the set of states of the automaton,

Σ – a finite set of input symbols,

$\delta=\delta(q,a)$ – Machine Transition Function (here $q \in Q$, $a \in \Sigma$),

$q_0 \in Q$ – the initial state of the automaton,

$F \subset Q$ – The set of the final states of the automaton.

When modeling a management agent as a deterministic finite automaton, the content and content of the tuple parameters (3.12) will be as follows:

Q – It is the set of states of a management agent. First of all, these are the characteristics of the gradations of the level of performance of his activities in solving a given problem. Thus, the condition of such an automaton is type 2AIA.

q_0 – initial state of the management agent (its state before the start of activity).

$F \subset Q$ – a set of final states of a management agent. This may be, for example, allowing him to continue his current activities (already at another stage of the development of a multi-stage project), the possibility (or expediency) of his transfer to another type of activity during the implementation of the project (for example, transferring him from an active position to a passive one, etc.), changing his personal task, withdrawing him from the project (for some period or altogether), etc. The set of final stages of the management agent is set by the project manager before it starts.

$\Sigma = \Sigma_1 + \Sigma_2$ – input alphabet, which consists of symbols describing the characteristics of Σ_1 (they are "programmed" by the management agent when choosing a strategy for carrying out activities) and motivational factors Σ_2 (they motivate the management agent to choose the strategies necessary for the optimal implementation of the activity). It is thanks to the perception of symbols from the alphabet Σ_2 is the transition of the management agent from one state to another. The

symbols of the alphabet Σ_1 affect only the level of efficiency of the activity. In fact, the alphabet Σ is an information space loaded with the purpose of activity.

$\delta=\delta(q_{i-1}\rightarrow q_i,a)$ – The function of the management agent's transition from one state (q_{i-1}) to another (the next one – q i). Most often, it is used in the transition from the previous stage of activity (for example, project execution) to the next (i.e., it is analyzed before the next stage, taking into account the state of the management agent at the previous stage).

The set of final stages of a deterministic finite automaton for a management agent must be decomposed into a direct sum of sub-states F_i, each of which corresponds to one or another method of its use in activity.

$$F = \oplus F_i,\ \forall i \neq j:\ F_i \cap F_j = 0 \tag{3.13}$$

If, before the next stage, the management agent is in the state $q_i \in F_j$, then his use in the further course of activity can develop only within the framework of this final state.

The main task when using the built model is to identify the current state of the management agent as a deterministic finite automation and to identify the function of transition between states inherent in this economic agent depending on changes in the economic situation.

The introduced deterministic finite autoation is a set of 2AIAs, which, in sequential order, carry out a given activity. The order of use of 2AIA is determined by the function $\delta=\delta(q_{i-1}\rightarrow q_{i,a})$. The achievement of the goal consists in reaching the final state F. This method of assigning the activity fixes the 2AIA that completes the activity. As a result, the application of the concept of deterministic finite automata is only a partial case of the use of 2AIA for control.

The method of constructing technologies for attributing a particular person to a certain class of characteristics of 2AIA activity is substantiated in detail and presented in [43,71,78]. Examples of the assignment of real people to a certain class of 2AIA and the results of the experimental study are given in [43,71,78,98-103]. The database of people was more than 1.5 thousand people [43,71,78]. A possible use of human physiological characteristics to determine the type is given in [104,105].

The scheme of the sensor for determining the class of activity of a given person is shown in Fig. 3.3.

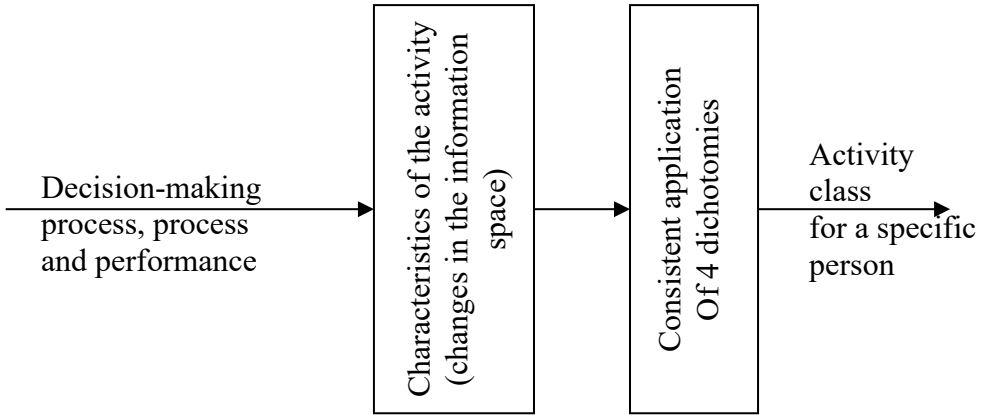

Fig. 3.3. Sensor for determining the class of activity for humans

The 2AIA classes, to which specific people were assigned, were often determined remotely, without contact with them (with the help of the media, other people's stories about them, biographical descriptions, etc.), which indicates the high effectiveness of the results obtained. A number of researchers have learned to identify classes of activities for people remotely, from texts posted on the Internet (for example, [43,71,78]) and without contact with the author of the dissertation, which indicates a high level of accessibility of the results obtained.

A detailed description of the results of assigning people to a certain class of 2AIA characteristics of the subject's activity and comparison of the set of classes of 2AIA and known psychological theories of personality is given in [43]. As analogues of the developed method for determining the class of human activity, only expert methods can be distinguished, but all of them, as a rule, are heuristic.

3.2 Model of protection of the subject of information security from negative information and psychological influence based on 2AIA technology

We will build a model of protection of a person as a subject of information security from negative information and psychological influence on the basis of the characteristic features of his activities. To do this, we will consider the channels of

information and psychological influence on the class of characteristics of the subject's activity, that is, on 2AIA, which can be represented in the form of a functional diagram of Fig. 3.4.

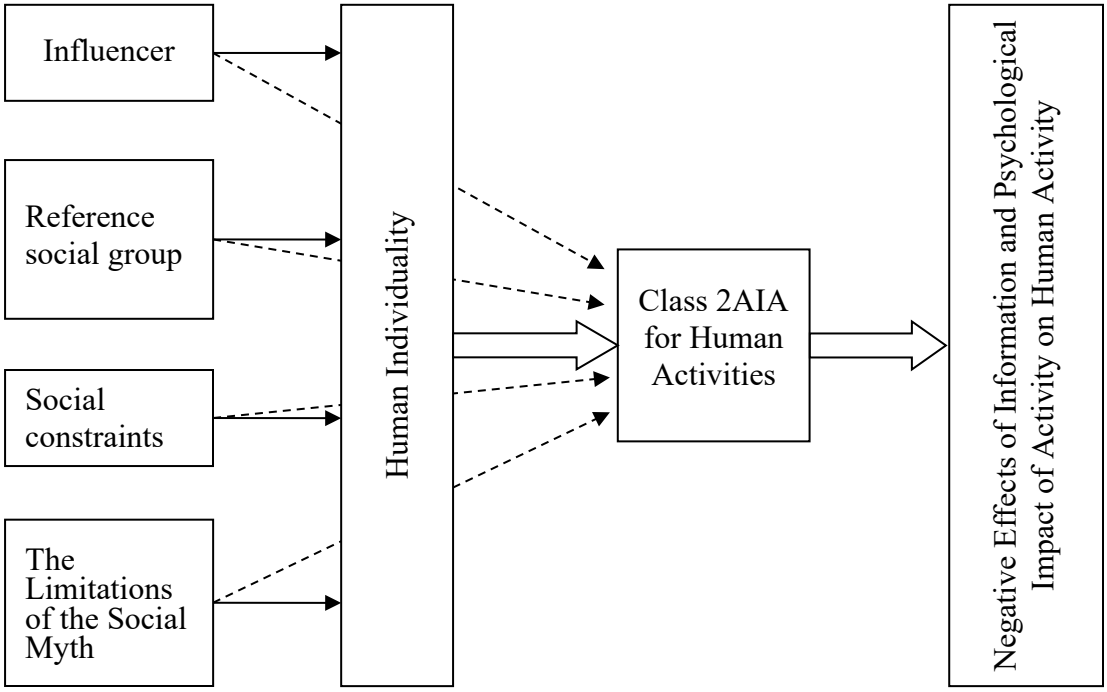

Fig. 3.4. Illustration of the process of protecting a person from negative information and psychological influence

Fig. 3.4 shows that the factors of negative information and psychological impact on a person are:

- agents of influence – i.e. individual subjects, to the information from which and the assessments of which the single subject takes into account when making decisions and carrying out activities;
- reference groups of subjects: social groups of subjects, to the information from which, norms and assessments of which the selected subject takes into account when making decisions and carrying out activities;
- restrictions of the external environment (social restrictions), i.e. acceptable and admissible in a set of subjects (society) methods, methods and algorithms of activity, assessment of permissible activities and decisions made;
- limitations of the social myth, i.e. acceptable and permissible in the set of subjects (society) goals of activity, types of restrictions on activity, etc.

Agents of influence are individual subjects of information security, which, as a result of communication with the subject in question, lead to the fact that it begins to carry out ineffective activities. They exert their influence both at the level of characteristics that characterize the individuality of a person, and at the level of the class of characteristics of the subject's activity (at the level of 2AIA).

A reference group of subjects is, as a rule, a set of subjects with which, as a rule, the subject in question seeks to identify itself. Therefore, the norms, ways and methods of action adopted in this group, factors that are ignored, etc., are all this the subject in question is trying to adopt. It should be emphasized that quite often the subject of information security has formed an inadequate opinion regarding those methods of activity and methods of communication that are accepted in the reference group of subjects (they are formed, for example, with the help of the media or feature films).

Social restrictions are actively formed in the subject of information security throughout his life, starting literally from birth. They form constraints on the methods of activity and communication during its implementation. For example, considering certain methods permissible only for very specific reference groups.

The limitations of the social myth belong to the worldview level and are formed, as a rule, at the level of the goals that the subject of information security "should" set.

All these factors affect the subject of information security, leading to inefficiency. At the same time, they can affect both the individuality of the subject and the class 2AIA of the characteristics of his activity (shown in Fig. 3.4 with a dashed line). It should be emphasized that if the characteristics of the subject, which describe his individuality, can sometimes be changed without a radical decrease in the effectiveness of his activity, then a change in the characteristics of class 2AIA of the characteristics of the subject's activity always reduces the effectiveness of his activity, and, in some cases, even makes it impossible.

The scheme of using the class of characteristics of the activity of the subject of information security for its protection from negative information and psychological influence is shown in Fig. 3.5.

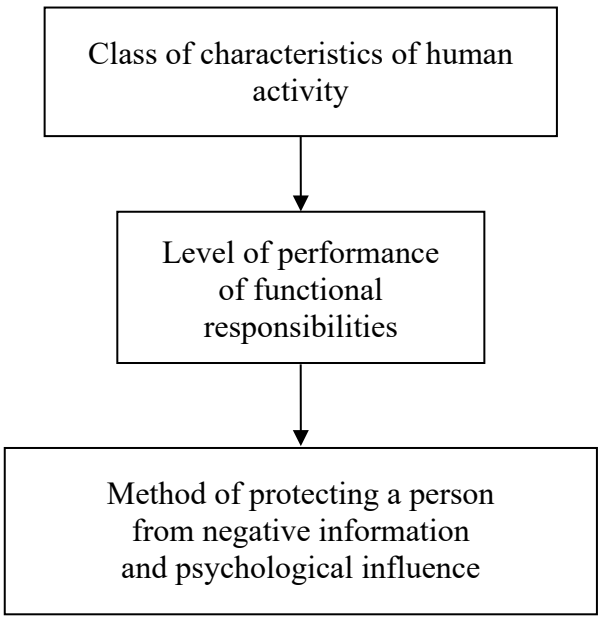

Fig. 3.5. The scheme of using the class of characteristics of human activity to protect it from negative information and psychological influence

The protection of the subject of information security from such negative information and psychological influence lies in the fact that the channels of such negative influence are blocked. Also, a very effective countermeasure is the implementation of analytical activities and the dissemination of their results.

The paper considers only those models and methods of protection of the subject of information security (person), which are based on the proposed set of 16 classes of characteristics of the 2AIA activity.

In order to protect the subject of information security from negative information and psychological influence, it is necessary to determine how he perceives and processes information, how he makes decisions and how he carries out activities [43,71,78, 98-101].

Above, a set of 16 classes of 2AIA was introduced, which allow you to carry out arbitrary activities in accordance with a given goal. Now it is necessary to establish the correlation between the introduced abstract concept – 2AIA – and a specific person.

Let us describe the structural construction of the method for determining (identifying) class 2AIA for management or activities for a specific person – that is, class 2AIA for a person.

The human being is a multifaceted object that is investigated from different perspectives within different scientific disciplines. Here we will consider a person as the most obvious candidate in order to describe him in terms of 2AIA. Therefore, it is quite legitimate to formulate the following task:

- To determine whether a particular person carries out such a class of methods, technologies, algorithms, ways, etc., to carry out activities that could be attributed to a certain class of 2AIA.

In order to be able to answer this question, it is necessary to develop a method for determining 2AIA in relation to humans.

First of all, let's describe the dichotomous method of determining the type of 2AIA.

It should be emphasized that each class of 2AIA is a class of related methods, technologies, algorithms, etc., for carrying out activities, the equivalence of which is set by their software and creative components. Therefore, in order to be able to consider a real object (a person) as 2AIA, it is necessary to investigate the ways of carrying out the activity that it uses.

To do this, it is convenient to apply the method of sequential dichotomous attribution of the totality of technologies for carrying out activity (the way it manifests its activity) used by this object to one of the alternative poles. The sequential application of four such independent dichotomies guarantees us that the object in question belongs only and only to one of the 2AIA classes. rice. 3.6.

Remarks. The dichotomous method is chosen only as one of the possible examples of the implementation of the general method for determining the class 2AIA.

The first dichotomy is based on the consideration of the software component of class 2AIA. It is based on differentiation between detailing and summarizing components of information for the 2AIA program block. Thus, a division is made into Generalizing classes 2AIA (generalizing classes of activity) and Detailing classes 2AIA (detailing classes of activity). This dichotomy describes, for example, how a real object expresses the purpose of its activity. It is given, in a certain sense of the word, by opposition – the opposition "sign – symbol" (or "part – whole").

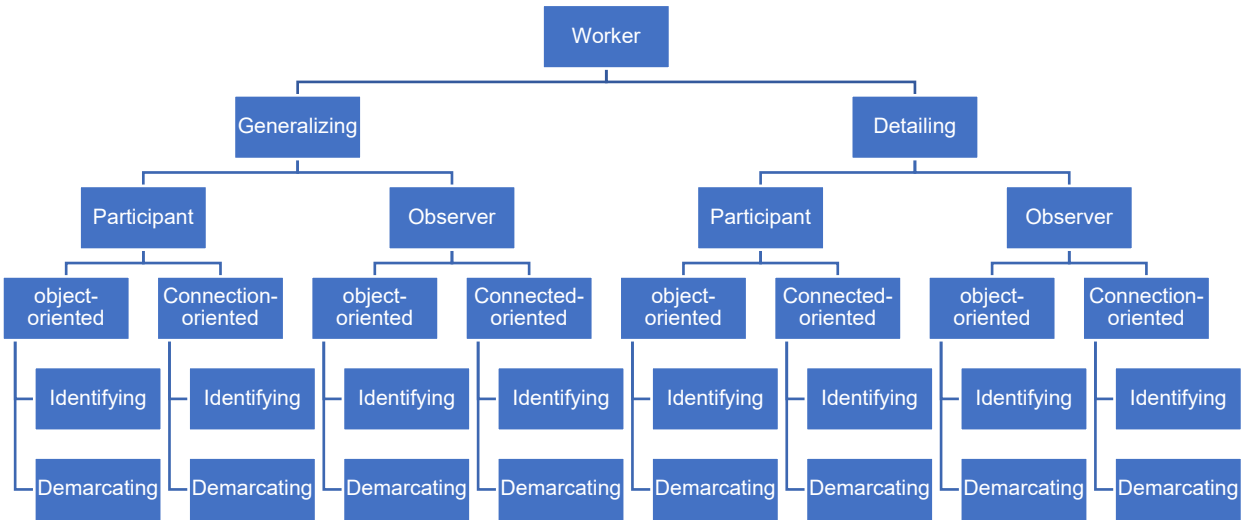

Fig. 3.6. Dichotomous distribution scheme

The second dichotomy determines the direction of the activity of this class 2AIA. Some classes of 2AIA, relying on the state, create processes. To do this, they are in a constant "creative process", in constant contact with those objects over which they exercise their control. Naturally, as long as they manage them. Such 2AIA classes will be referred to as Participants. Other 2AIAs, being programmed by a process, create a state. They will be called Watchers. Thus, this dichotomy makes the division of 2AIA classes into Participants and Observers. It is defined, in a certain sense of the word, by the opposition "process-state" (or "statics-dynamics").

For the third and fourth dichotomies, the location of the relevant components of information does not matter. They can belong to both the program block and the creative block of this 2AIA.

The third dichotomy determines whether single real objects are used in the process of activity, or whether the activity is described in terms of many single real objects. Activities that are described only within the framework of single real objects will be called Object-oriented. Activities that are described within the framework of many single real objects are what we will call Connection-Oriented. It is given, in a certain sense of the word, by opposition – the opposition "one – many (totality)".

The fourth dichotomy determines whether the structure of the entire hierarchical level (the structure of a set of objects) is used in the process of activity, or whether management is described in terms of the boundaries of the hierarchical level as a whole. In the first case, we will use the name Identifying for this class

2AIA. In the second – Demarcating. It determines, in a certain sense of the word, opposition – the opposition "identity – difference" (or "identical to me – different from me").

It should be noted that in the real case, the activity described as class 2AIA can be applied to arbitrary objects that may not be hierarchical systems. Then the detailing component of the information is a set of data on the individual characteristics of real objects. And the generalizing component of information is a set of information about the "general" properties of a certain class to which the real object in question belongs.

A person, as an object for the use of the 2AIA apparatus, is considered exactly to the extent that he or she carries out independent and conscious activity. The following "working definition of a person" can be given based on this point of view:

1. A person is considered as an object that implements a given set of technologies (ways, methods, ways, modes, algorithms, etc.) to carry out activities. "The class of characteristics of human activity is class 2AIA." It is this and only this aspect of human activity and activity that the 2AIA apparatus describes.

This interpretation of data on activity is the basis of a method for determining the class of activity that a person performs.

It is in this sense that we will henceforth use the term "class of activity (management) for man" (=2AIA). Or, abbreviated, "person class" (or "person class" – when referring to a specific person).

The purpose of the method for determining the class of a person is:

- Attribution of a set of technologies (ways) of carrying out the activity of a particular person sequentially to the corresponding pole of each of the 4 possible dichotomies.

Let's give an explanation of what has been said, going down one logical level, considering the hierarchical (according to the level of complexity) structure of the proposed methodology:

Structure of the method (supporting elements):

1) From a particular person, we need information about how he organizes his activities when he encounters something new, how this new is processed by a person,

2) identification of several areas of human activity where the choice of management is carried out alternatively, 3) A way to highlight some of the answers as uninformative.

Method boundary (sorting "unnecessary" and "uninformative"):

1) how exactly a real person carries out the process of highlighting the new (Generalizing – Detailzing),

2) the limits of the applicability of the methodology (it should be clearly described that the type of person is not a psychological type of individuality, but a described orientation towards a certain group of people – this is especially important for the correct choice of questions and areas of activity),

3) "What do I expect from others" and "What do I personally want to do" – taking into account and dividing (for people with a certain class of activity).

Individual elements of the method:

1) blocks of questions (descriptions of human activity), within a certain dichotomy;

2) nested blocks of questions (descriptions of human activity) within one area of human activity.

3.3 Features of the development of amethod for protecting the subject of information security from negative external influence in the tasks of information and cybersecurity

The peculiarity of the development of amethod for protecting the subject of information security from negative external influence in the tasks of information and cybersecurity is that a person, i.e. The subject of information security, under the influence of various external negative factors, can turn into a threat agent and cause damage to even the most modern cybersecurity system, both consciously and unconsciously, since a full range of cybersecurity systems has not yet been developed that would completely exclude the human factor [05].

Therefore, in order to develop a method for increasing the protection of the subject of information security (a person) from negative information and psychological influence, we will consider the tuple that describes the class 2AIA T [43,64,71-81].

$$T =< C_{in}, C_{out}, AS, G, C > \quad (3.14)$$

Here, C_{in} is the component of information at the entrance to class 2AIA of the subject's activity; C_{out} – information component at the output of class 2AIA; AS – subject area of activity; G – purpose of the activity; C – a set of restrictions that are imposed on the choice of goals of activity, methods of information processing (for example, building an information space), methods of carrying out activities, etc.

According to the model of subsection 3.2, a negative informational and psychological impact can be exerted on each of the elements of this tuple or on a certain combination of them. The factors of such influence and the channels of its implementation are shown in Fig. 3.4.

The implementation of a negative informational-psychological influence on an arbitrary element of the tuple T_k can be described by the operator N, which acts as follows.

$$N : T_k \rightarrow T_k^a . \tag{3.15}$$

In (3.15), the index "a" indicates that the element of the tuple T_k has changed.

In general, there can be two different cases:

$$\exists t_j (t_j \in T_k : t_j \notin T_k^a) \tag{3.16}$$

and

$$\exists t_j (t_j \notin T_k^a : t_j \in T_k) . \tag{3.17}$$

Case (3.16) corresponds to the situation when, as a result of external informational-psychological influence, one of its "correct" components t_j is removed from the element of the tuple Tk.

Case (3.17) corresponds to the situation when, as a result of external informational-psychological influence, a new "incorrect" component t_j is added to the element of the tuple Tk.

The case when one "correct" component of the tuple element T_k is replaced by an "incorrect" one is reduced to the sequential application of operations (3.16) and (3.17).

The process of protection of an individual subject of information security $Si = CS$ is shown in Fig. 3.7.

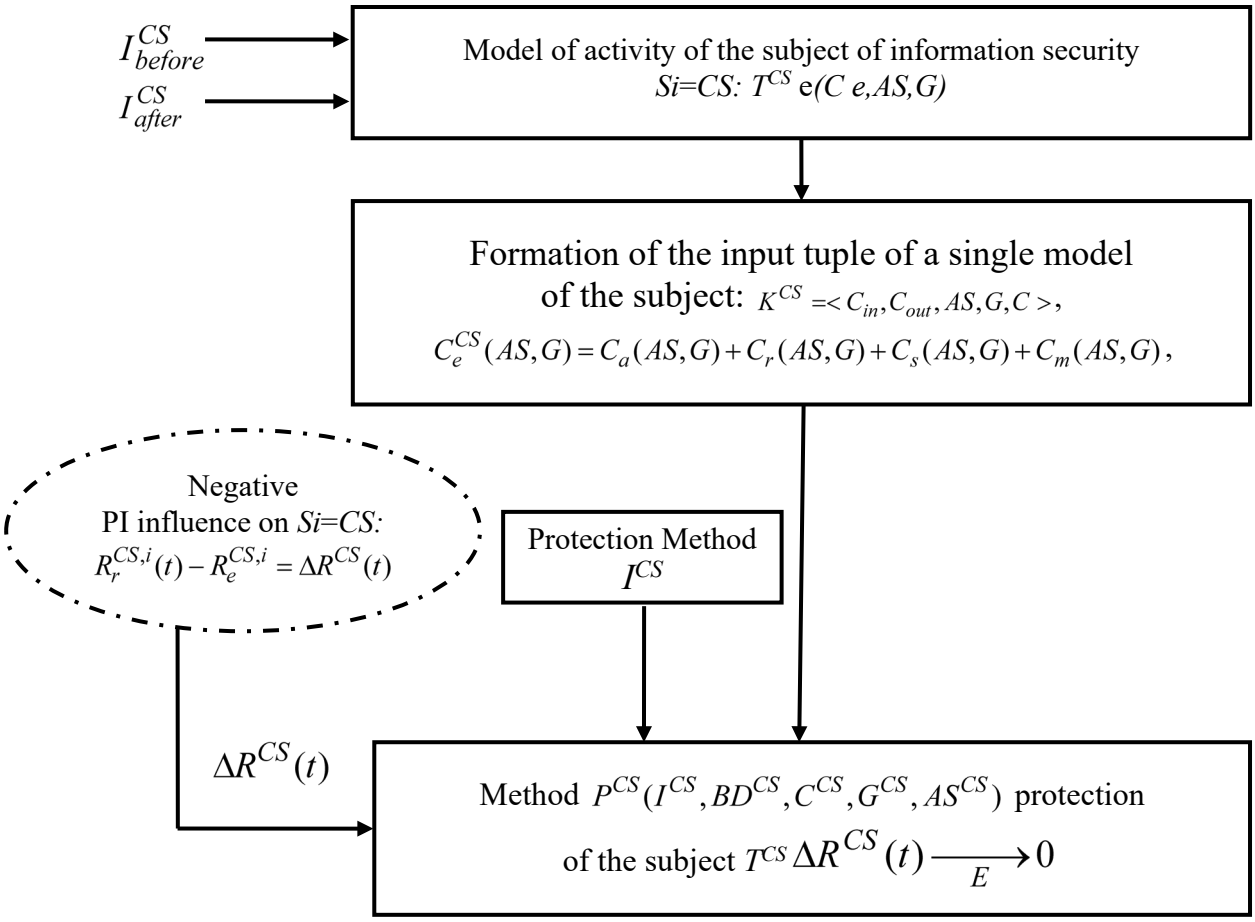

Fig. 3.7. The process of protecting an individual subject
of information security Si=*CS*

The method of protecting a person as a subject of information security from information and psychological influence using class 2AIA of the subject's activity can be presented in the following form.

Stage 1. A theoretical (exemplary) database (database for samples) T_e for each of the 2AIA classes for different subject areas of activity is created using the subject's activity model.

Stage 2. A database is created for restrictions on the activities of the subject C $_e$, which are characteristic of the interior of the activity where the subjects under consideration will carry out their activities. These constraints include the restriction of the agents of influence C a, the restriction of the reference groups $_{Cr}$, the social constraints of C $_s$, and the constraints of the social myth C_m. In some cases, each of these constraints may depend on both the subject area of activity *AS* and the purpose of activity *G*. In other words, the created database has the following structure:

$$C_e(AS,G) = C_a(AS,G) + C_r(AS,G) + C_s(AS,G) + C_m(AS,G). \qquad (3.18)$$

Formula (3.5) specifies the breakdown of constraints, i.e.

$$C_a \cap C_r = C_a \cap C_s = C_a \cap C_m = C_r \cap C_s = C_r \cap C_m = C_s \cap C_m = \varnothing. \quad (3.19)$$

When writing (3.6), it is taken into account that different groups of constraints belong to different hierarchical levels of description of factors influencing the subject, and therefore they do not have common elements.

Stage 3. For each subject area of activity and for each purpose of activity in it, taking into account the restrictions of activity characteristic of this subject, a database of samples *T* e*(C e,AS,G*) is created on the basis of a theoretical model for the characteristics of activities of class 2AIA in a given subject area and for the fulfillment of a given goal.

Stage 4. For class 2AIA of the activity of a given subject, one element is selected from the database *T* e*(C e,AS,G*)

$$T_e^i(C_e, AS, G) \in T_e(C_e, AS, G), \qquad (3.20)$$

which corresponds to its activity class 2AIA. At the same time, the purpose of the activity, the subject area of activity (interior of the activity) and the restrictions characteristic of this subject are taken into account.

Thus, for each subject, an approximate database of the results of its activities is set

$$R_e^i(t_e^i, C_e, AS, G). \qquad (3.21)$$

Stage 5. The real current state of the results of the activity of a given subject at time *t* is determined

$$R_r^i(t). \qquad (3.22)$$

Stage 6. A comparison is made by the components of the tuple (3.14) of the approximate database of the results of the activity of the subject R $_e$ i with the real results of the activity of the given subject $R_r^i(t)$ at time *t*.

If, as a result of the comparison, equality is obtained

$$R_r^i(t) - R_e^i = \varnothing, \tag{3.23}$$

then the act of negative information and psychological influence did not take place. In this case, the level of protection of the subject of information security is sufficient.

If there is such a ratio

$$R_r^i(t) - R_e^i = \Delta R(t) \neq \varnothing, \tag{3.24}$$

then this means that you need to move on to the next stage.

Stage 7. It is necessary to analyze the reasons for the appearance of changes in $\Delta R(t)$ in the set of results of R_e^i activity.

If the reason for the change in $\Delta R\ (t)$ results was an objective change in the situation, then it is necessary to:

1) either move on to stage 1, again building on the basis of the model of activity of the subject of information security a new database of exemplary results of its activities R_e^i, which correspond to the new objective of activity G and changes in the subject areas of *activity of SA;*

2) or develop *measures to* counteract the identified negative information and psychological impact. The objective function of such activities can be defined as follows.

$$\Delta r(t) \xrightarrow[E]{} \varnothing \tag{3.25}$$

Note that points 1-3 are carried out once, and then you can use the *database* $T_e(C_e, AS, G)$ for a long time and for a large number of people. Thus, this base has a high level of versatility.

The proposed method of protecting a person from negative information and psychological influence uses the proposed model of structuring the information space of individual subjects to protect against influence, as well as dividing the set

of characteristics of activity into subsets with characteristics characteristic of a wide range of subjects and an individual subject, allocating the characteristics of the subject's activity from 16 defined classes (classes are distinguished by the poles of the dichotomies "participant – observer", "generalizing – detailing" and others), which made it possible to identify factors, channels and characteristics of negative information and psychological influence on an individual subject.

The following set of criteria has been developed to assess methods of protection of the subject of information security from negative information and psychological influence: the level of justification of the model for the subject's activity; the level of consideration of the negative information impact on the subject; the level of completeness and sufficiency of the model of human activity; the level of use of types of activities for subjects; the level of consideration of the influence of the social environment; the level of use of objective characteristics of activity; success rate in forecasting decision-making by the subject; the level of adequacy in forecasting decision-making and activities by the subject; the level of information influence on the subject of channels depending on the type.

Previously, in order to identify the negative information and psychological impact and to counteract it, the use of these characteristics of the activity of a particular subject in a "mixed form" was used, which led to the fact that:

1) it was necessary to create an appropriate database for each specific subject, as a result of which the number of such databases became too large, and the cost of their creation was too high, which made it impossible to use them widely to protect the subject from negative information and psychological influence;

2) it was not possible to distinguish the characteristics according to the level of their importance for the results of the subject's activity, which led to the "clogging" of databases with characteristics that were not important for use in the tasks of protecting the subject from negative information and psychological influence;

3) the creation of such databases required highly qualified employees, and the creation of the databases themselves took a fairly long period of time;

4) it was impossible to create effective decision support systems for the use of such databases, because each use of these databases was unique and could be transferred to another entity.

The use of 2AIA classes for the activities of the subject of information security made it possible to divide the database – the set of characteristics of the activity of the subject Ch – into two subsets: a subset of the characteristics of the individuality of a particular subject Ch $_i$ and a subset of the type characteristics of the activity of this subject Ch_t:

$$Ch = Ch_i + Ch_t, \quad Ch_i \cap Ch_t = \varnothing \tag{3.26}$$

This made it possible to structure the channels of negative information and psychological influence, and led to an increase in the protection of a person from negative information and psychological influence due to the allocation of universal characteristics of their activities for a wide range of subjects.

A comparison of the existing methods of protecting the subject from information and psychological influence is given in Table 3.1. It shows that the proposed method, unlike the existing ones, includes a model of the subject's activity. This makes it possible to forecast the results of its activities in new conditions. Unlike the existing ones, the proposed method uses only objective characteristics of the process and result of human activity, and forecasting is also carried out in such characteristics. To determine the level of efficiency of using the proposed method of protecting a person from negative information and psychological influence, it is proposed to compare it with existing methods – analogues. To accomplish this, methods of expert evaluation can be used [36,58].

Modern models and methods of information security are usually focused on the description of information security objects [4,107-111]. The subjects of information security are considered in them within the framework of the implementation by the subjects of clearly defined rules for decision-making and the implementation of activities. However, people, as subjects of information security, as a result of information and psychological influence from other subjects, often make decisions and carry out activities that may differ from those required by information security models and methods (this was most clearly manifested within WikiLeaks [2]).

Table 3.1. Comparison of the characteristics of the developed and existing methods of protecting a person from negative information and psychological influence.

№	Characteristics of the method	Psychological methods	Sociological methods	Management methods	Proposed method
1	Level of justification of the method: causal; statistical; heuristic (expert); forecast and forecast verification.	 – +/– +/– –	 – + + –	 – + + –	 + – – +
2	To apply the method, a model of the subject is required	+	+	+	–
3	The method incorporates a subject model	–	–	–	+
4	The method uses the characteristics of all subjects	+	+	+	–
5	The method uses the characteristics of an individual subject	–	–	–	+
6	Use performance characteristics	–	–	–	+
7	The method makes it possible to make a forecast in new conditions for the subject	–	–	–	+
8	Allows you to predict the impact on the subject of his social environment	–	–	–	+

To describe the activities of subjects (first of all, decision-making and management) in the tasks of information security, specialists are forced to use, as a rule, models and methods that are based on management, sociology and psychology.

3.4. Conclusion to Chapter 3

1. For the first time, the model of structuring the information space of the activities of individual subjects of information security is used to apply in the development of a method of protecting the subject from information and psychological influence. It is proved that arbitrary activity in the information space can be described by two-component operators, which translate one component of the information space, which describes the subject area of activity before the implementation of the activity, into one component of another information space, which describes the subject area of activity after the implementation of the activity.It is proved that in order to describe arbitrary activity in the subject area of the task, it is necessary, in general, to have 64 two-component operators that translate the information space "before the activity" into the information space "after the activity". It is shown that simple regulators and systems of positive and negative feedback can be described as certain such operators.

2. For the first time, a division of the set of characteristics of activity into subsets with values of characteristics of the subject's activity inherent in a wide class of subjects has been carried out. It is proposed to divide the set of characteristics of the results of the subject's activity into 16 classes (subsets), each of which describes a two-component abstract information automaton (2AIA). Separate classes differ according to the poles of four dichotomies: "Generalizing – Detailizing", "Participant – Observer", "Connection-oriented – Object oriented" and "Identifying – Delimiting".

3. A method of protecting a person from negative information and psychological influence isproposed, which uses the proposed model of structuring the information space of individual subjects to protect against influence, as well as dividing the set of characteristics of activity into subsets with characteristics characteristic of a wide range of subjects and an individual subject, allocating the characteristics of the subject's activity from 16 defined classes (classes are distinguished by the poles of dichotomies "participant – observer", "generalizing – detailizing" and others), which made it possible to identify factors, channels and characteristics.

CHAPTER 4 MODELS AND METHODS OF INFORMATION SECURITY IN SOCIAL NETWORKS

4.1. Model of information security of social networks taking into account the peculiarities of information interaction of agents

Social networks are made up of subjects and objects, i.e. human and computer components, as well as artificial intelligence components and automatic control systems.

As shown in Chapter 3, some of the components of artificial intelligence and automatic control systems can be described within the framework of AIA. In the future, only networks consisting of 2AIA will be considered, because this makes it possible to use the results obtained in the dissertation as fully as possible.

The structural and functional model of protection of the subjects of information security and the social group from negative information and psychological influence is presented in Fig. 4.1.

The information space of the subjects' activities can be built both in a one-level approximation and in a multi-level one. Single-level is used in the construction of 2AIA protection models and in models of protection of one-level social networks from negative information and psychological influence. The multi-level information space is used to improve the security of multi-level social networks and to model the role of coordinators in the protection of the subject of information security and social groups.

Classes 2AIA are used to protect a person as a subject of information security and to model the joint activities of people. The set of binary relations between 2AIA classes is used to protect the subjects of information security and social groups and to model the functioning of social networks. Game theory, which creates models and methods for coordinating interests between information security actors, is used to protect single-level and multi-level social networks.

All these models and methods are part of the system of information and psychological security of a person and a social group.

For the successful solution of management problems, direct integration into the decision-making subsystem of such databases and knowledge (DB/Z), which contain a model of the corresponding fragment of the picture of the real world in which management is carried out, is required. This also includes the need for the existence of a model of the subject of management itself. The need for this is caused by the fact that the model, as a system for compressing information about the controlled object, defines the entire class of admissible solutions.

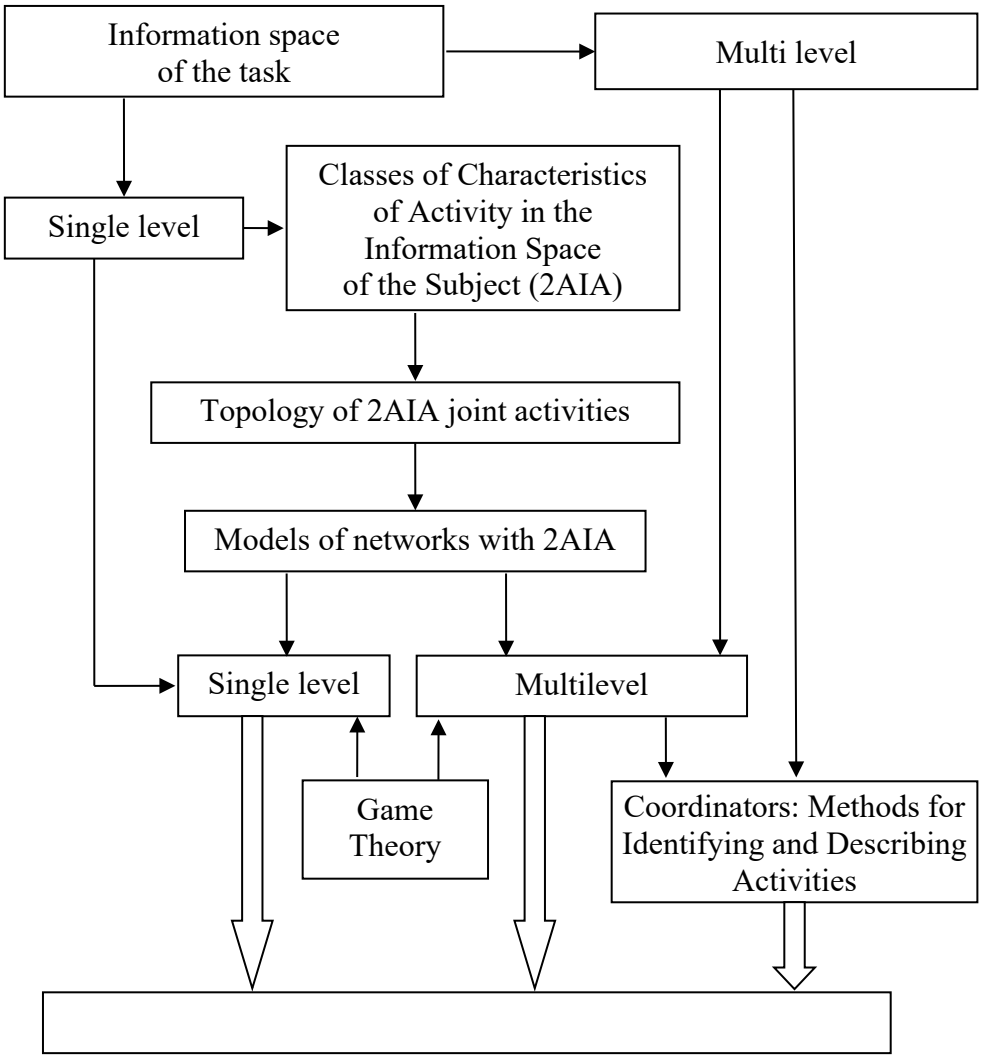

Fig. 4.1. Structural and functional model of protection of subjects of information security and social group from negative information and psychological influence

Unfortunately, this circumstance is not always recognized by analysts and decision-makers. Most often, they simply do not see the point in building a visual and adequate model of the fragment of the real world in relation to which management decisions are made. As a result of the rejection of the objective parameterization of their management settings, which affect the parameters of management, their decisions cannot claim the status of justified and enter the control loop, having the status of a hypothesis, the possible nature of which is most often not realized and, therefore, is not controlled by the manager [4-6,36,40,43,46,48,78]. Such a situation poses a threat to the integrity of the object and the subject of management, since the system formed by them is used as a simulation model, the input of which is given such a test effect that has a perturbation.

This is especially evident in automated control systems (ACS). In modern automated control systems, the stage of compressing data/knowledge into concepts-terms is entrusted, as a rule, to a person: that is why it is the most inertial link [4-6,36,40,43,46,48,78,90]. The construction of databases/knowledge on the basis of which management and activities are carried out reflects either the logical structure of the management algorithm, or the technologies initiated by it, or simply the personal preferences of the expert [49,50]. Almost always, databases/knowledge bases are tightly coupled deterministic systems.

The technology of building a network multi-level structure for managing production and organizational systems, which has the properties of self-learning, fractality, holography, and associativity, is described below. Databases/knowledge that meet certain requirements, at the same time, are blunted as a necessary component. The theoretical and mathematical apparatus that allows synthesizing multi-level management structures of production and organizational systems of arbitrary level, which have the properties specified by the customer, is described.

The class of problems that can be solved with the help of the multi-level structures of management of production and organizational systems described in the work coincides with the class of problems that are solved in the field of management of both an individual subject of information security and structured management systems of arbitrary complexity and hierarchical structure.

First of all, let's dwell on the terminology used. In this, we proceed from the results [53,71,78].

Definition 4.1. Database/Knowledge Base (D/KB) is a single "text" divided into fragments (elements, nodes) and connected into a single whole by a system of cross-references. The D/KB stores activity programs, norms and models of behavior, and interactions between control agents that are significant for management purposes.

The database/knowledge base, due to objective and subjective constraints, is divided into a system of fragments [53,71,78]. Constraints can most often be the characteristics of information "capacity" and bandwidth of data input/output channels, as well as the amount of memory (for example, for a specific individual). In this case, D/KB is split so that each of its fragments does not exceed the permissible values.

A single fragment of D/KB (text or sign) is not able to accommodate an integral system of knowledge sufficient for the implementation of management. Therefore, each D/KB is overgrown with stakeholders (decision-makers), specific

organizational structures, and mechanisms for transferring knowledge from this database to new databases/knowledge bases (to new knowledge carriers).

All this set of mechanisms that ensure 1) the continuity of the database and 2) the fragmentation (restructuring) of the database into separate fragments does not belong to the D/KB itself. It is a separate "translation mechanism" between different D/KBs. The D/KB formed in this way is a certain "distributed program" for solving a certain class of problems of managing a certain class of objects (general knowledge is divided into fragments, the carriers of which are the elements of D/KB). This D/KB system has an external "system of rewriting" knowledge to "new media" (i.e., new elements of the aggregate database/knowledge).

Thus, the problem of constructing D/KB becomes equivalent to the task of constructing such a structure D/KB that is able to solve the whole complex of problems for managing a given class of objects under given conditions. This is achieved by creating links between the specified D/KB information elements and the control complex and the links between them.

The solution of this problem can be based on different methodological approaches. The dissertation proposes one of them, which is based on the following statement:

- The structure of D/KB should reflect the characteristic features of the organization of the decision-making process both by an individual entity and by organizational systems of different levels of hierarchy.

Considering D/KB as a variety of model objects, we introduce the term "path" in a standard way [71,88].

Definitions 4.2. A path in D/KB is an ordered set of nodes that are connected to each other.

In other words, a path in D/KB is a fragment (main part) in the decision-making and decision-making algorithm, which, in fact, turns D/KB into a certain program of actions.

This makes it possible to use the notion of a fundamental group as a characteristic of D/KB, and, as a result, the topological characteristics of the structure of D/KB according to the standard procedure (see, e.g., [88]). Databases/knowledge bases can be classified using their topological properties (i.e., by their topological characteristics). In particular, the concept of homotopy equivalence D/KB can be introduced (see Homotopy Equivalence D/KB).

Moving on to the interpretation, we can say that each hierarchical D/KB is a hierarchically organized fractal system of nodes-concepts (texts, fragments). At the

same time, the term "fractal" is understood as "self-similar" in a generalized sense (see the description of fractal characteristics of objects [78]). Some of these nodes are combined into closed paths, which pass, in general, through several hierarchical levels. As a result, we get a certain universal and self-consistent description of a certain piece of knowledge – in this sense, we can say that such a definition is true.

Definitions 4.3. The closed-loop invariance class in D/KB defines (specifies) the control class that can be carried out with the help of such a D/KB (i.e., defines a certain fragment of the World Picture).

In this case, the Picture of the World, which is "compressed" in this D/KB, can be characterized by parameters that describe the topological structure of this database/knowledge itself.

D/KB as an element of the control system are open in the sense that they carry out the process of "translating" the information that comes to the "input" of the D/KB to the control commands at the "output" from the D/KB.

The process of management optimization will then take place according to the following generalized algorithm: compression of information → Entering information into the D/KB → Movement of information along the path through the D/KB → Output of information from the D/KB → Implementation of management → Entering information into the D/KB → and so on.

Since in the "external" world (in relation to D/KB) control is also carried out by means of certain paths ("chains of control", – – see more in [53,71,78]), we come to the need to consider two different types of paths.

Definition 4.4. An internal closed path passes only through nodes of the same D/KB.

Definitions 4.5. An external closed path contains nodes (objects) that do not belong to the D/KB of the same (some nodes belong to the outside world.

In relation to D/KB, the concept of "learning" can be defined as follows.

Definitions 4.6. Learning in relation to D/KB is the process of consolidating pathways in D/KB, both internal and external.

The D/KB learning algorithm is similar to that of neural networks.

The D/KB nodes through which information is input/output to D/KB have specific properties. The following definition can be given.

Definitions 4.7. The interfaces between internal and external D/KBs are those D/KB nodes that have the property of exchanging information (data) between D/KB and the outside world.

In [58,64,71] it is shown that the structure of many production and organizational systems and objects can be described in a universal way. As a result, it is possible to introduce the concept of "internal model of the world", understanding by this a set of characteristics of the topological structure D/KB, and the concept of "external model of the world", understanding by this the topological structure of the description of a given class of problems about the control of the object, for the control of which this D/KB is created.

Using the results of Section 4, it is easy to show that D/KB is given by its topological parameters (i.e., D/KB are classified according to the parameters that characterize their topological structure). As a topological parameter that characterizes D/KB, a fundamental group for the set of their internal paths can be chosen.

Statement 4.1. In order for D/KB to be an adequate model for controlling the external world, it is necessary that the topological parameters that characterize the internal paths in D/KB (i.e., the "internal picture of the world" recorded in it) coincide with the topological parameters that characterize the external world (i.e., the controlled object).

Proof. The topology of internal paths in D/KB defines the system of activity chains and feedbacks that are used in management. The entity management model of the outside world can also be reduced to chains of control and feedback. In the event that these chains and feedbacks do not coincide, it will not be possible to achieve effective management.

Thus, databases/knowledge bases are built as a kind of "reflection" of the managed object.

It should be noted that management is always (at one stage or another) carried out through the mediation of the subject of activity, that is, the human operator. If we consider complex systems, then to manage them it is necessary to involve large, as a rule, hierarchically organized, managerial groups of subjects. In this case, the possibility of effective management is limited by how fully the parameters that characterize the managerial specifics of such groups are reflected in the D/KB. Thus, we come to the following statement: D/KB has an optimal structure when it corresponds to the structure of the group of subjects that carry out management.

The issues of implementation of optimal management in production and organizational systems have already been considered in detail in the dissertation earlier, where the classification of classes 2AIA of the characteristics of the activity

of the subject of management has been developed. In particular, such a statement was proved there.

Statement 4.2. The construction of activity (control) characteristics on the set of all possible classes 2AIA, which is able to optimally transform new information and develop and implement a new solution, is in the topological sense homotopically equivalent to a bouquet of 6 circles, or diffeomorphic to a two-dimensional sphere with 7 Möbius films glued in).

From this statement and the results of Section 4, the following statement follows.

Statement 4.3. At any hierarchical level, the D/KB of optimal structure is a set of connected internal paths that are oriented to certain fragments of the picture of the external world (control objects). The topological structure of such systems is diffeomorphic to a closed two-dimensional sphere with 7 Möbius films glued in, or homotopically equivalent to a bouquet of 6 circles. The value of the Euler index for this topological construct is χ=-5.

The structure of the described D/KB is discussed in detail in [64,71,78], where a theorem that can be formulated in the form of the following statement is proved.

Statement 4.4. The link graph of the D/KB nodes is 7±2 (Miller's number).

This statement follows from the results of Chapter 4. It differs only in that some D/KBs will be used in automatic mode during driving. This makes it possible to cover a wide class of human-machine systems within the framework of a single approach, from a single point of view.

Thus, D/KB is transformed into a network that has fractal (self-similar) properties.

The process of learning in the implementation of management is described as follows: D/KB learning is the processes of 1) transforming a node into an interface (or an interface into a node), and 2) forming and consolidating new paths (both internal and external) that run alone, sequentially or in parallel, as well as their destruction.

Ultimately, the following statement follows from the consideration carried out.

Statement 4.5. Optimal management of an object (including a production or organizational system) can be carried out only with the use of such D/KB, which have the following properties: 1) D/KB plays the role of a distributed program of

activity (part of which belongs to information technology, and part to the subjects of activity, i.e. human operators), 2) D/KB has associative, holographic and fractal properties.

D/KB should be activity programs because they (its components – nodes and links) should actively participate in the decision-making process enshrined in the definition given earlier.

D/KB must have fractal properties because, firstly, at each of the hierarchical levels their structure must satisfy the same regularities, and, secondly, its nodes will form a certain self-similar structure, the structure of which is described in statement 6.3.

D/KB must have holographic properties, understanding by this its ability to function efficiently in the event of a failure of even a sufficiently large number of its nodes and connections, since it has an excessive number of closed paths (both internal and external).

D/KBs must exhibit associative properties, understanding by this their ability to respond 1) "by analogy" and 2) to a previously unknown stimulus. This is due to the fact that the presence of different pathways between the "receptors" and "effectors" of D/KB (between its interfaces) ensures that there are a sufficient number of heterogeneous solutions.

Thus, it follows from the analysis that the proposed structure of D/KB allows to transfer to automated systems the solution of a part of those classes of tasks in the field of management, which were previously available only to an individual subject of activity or management (i.e. a human operator) or a group of subjects (operators).

4.2. Method of protecting single-level social networks

A social network consists of individual subjects of information security, which are interconnected by a communication system created by people on the basis of common preferences in communication and profitability in joint activities (the latter is mainly professional social networks).

To build a method for protecting a one-level social network (OSN) from negative information and psychological influence, consider the following tuple.

$$OSN =< G, T, IR, St, AS > \tag{4.1}$$

Here, *G* is the purpose of OSN functioning; *T* is a set of classes 2AIA of the characteristics of the activities of information security entities that make up OSM; *IR* is the set of binary relations between the 2AIA classes in OSN; *AS* is a set of subject areas of activity for the entities that make up the OSN.

The process of protecting a one-level social network from the negative impact of *Si=OSN* is shown in Fig. 4.2. Explanations in the text of the dissertation.

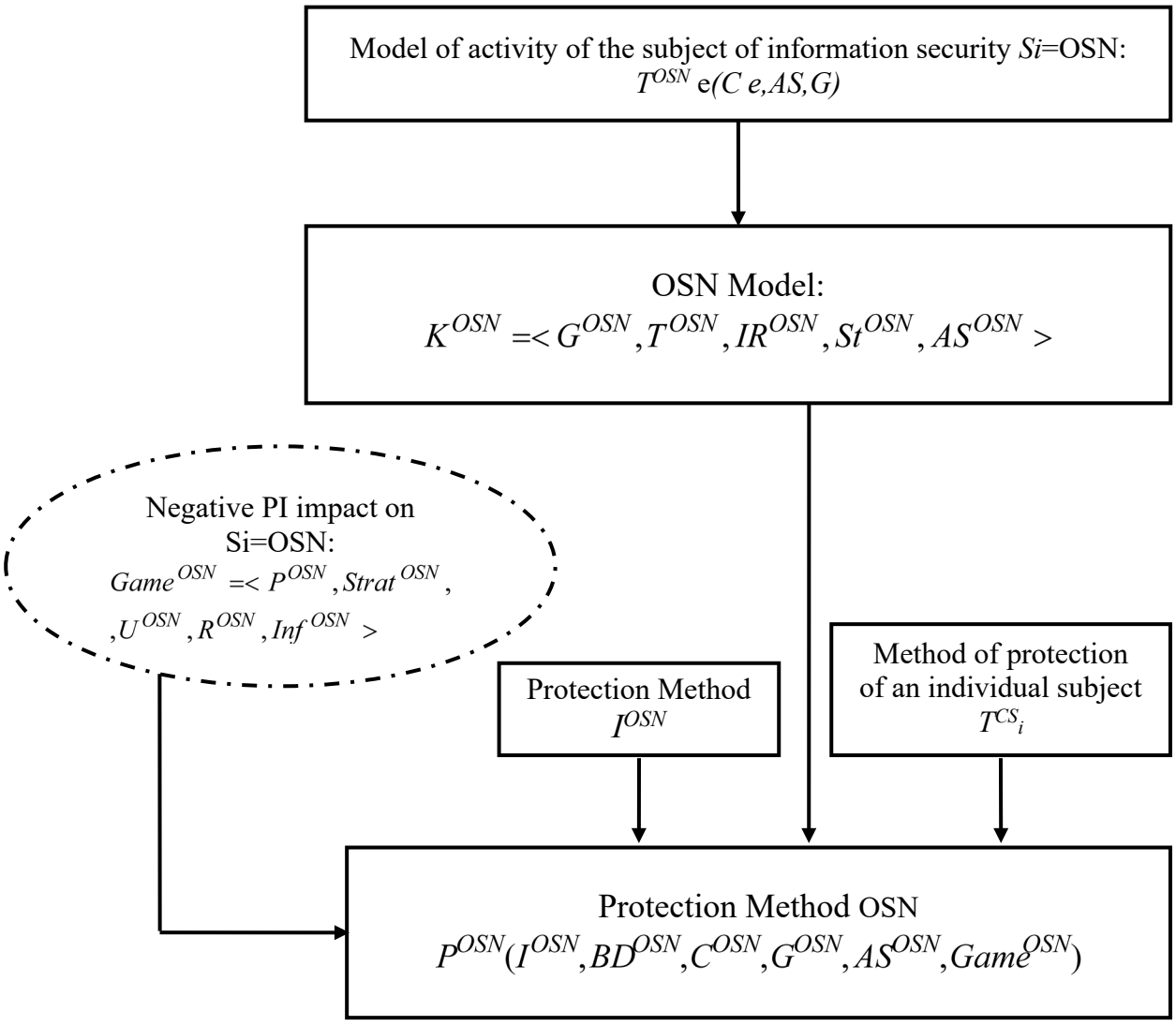

Fig. 4.2. The process of protecting a one-level social network from the negative impact of Si=OSN

The method of protecting OSN from negative information and psychological influence can be presented as follows.

Stage 1. The set of *T* classes 2AIA of the characteristics of the activities of the subjects of information security, which make up the OSN, are determined.

Stage 2. For each of the subjects of information security (OSN agents) with the appropriate class 2AIA $t_{and} \in T$, protection against negative information and psychological influence is carried out according to the method presented in subsection 3.3. When applying it, it should be taken into account that the goal of negative information and psychological influence can, in some cases, be goal G for OSN as a whole.

Stage 3. For each i-th agent belonging to the corresponding class 2AIA, we define the set IR_i of its binary relations with other agents with which it is connected in the network as with the corresponding classes of 2AIA. Protection of this agent from negative information and psychological influence is carried out according to the method presented in subsection 4.2, taking into account, if necessary, the subject area of activity of AS $_{and}\ AS \subset$ for this agent (subject of information security).

Stage 4. We define all possible structures that can be built on OSN, considering it as a graph in which the 2AIA classes act as nodes and binary relations as arcs. This way of representing a 2AIA network is described in Section 4.1, where symmetrical relationships are represented by edges and asymmetric relationships by arcs. The elementary structures are the rings of individual and dyadic self-programming, as well as the socion. Detailed examples of the application of this step are given later in this subsection.

Stage 5. In the case when there is a need to coordinate the interests of the parties in the implementation of OSN activities, in order to increase protection against negative information and psychological influence, it is necessary to improve the theory of games by taking into account the characteristics of agents' activities in the 2AIA classes. This improvement is made later in this subsection.

The following set of criteria has been developed to assess methods of protection of a one-level social network from negative information and psychological influence: the level of justification of the model of activity of the OSN agent; the level of consideration of the negative information impact on the OSN agent; the level of completeness and sufficiency of the model of activity of the OSN agent; the level of consideration of the types of agents' activities; the level of consideration of the influence of the social environment on the OSN agent; the level of use of objective characteristics activities of an OSN agent; the level of adequacy in forecasting the decision-making and activities of the OSN agent; the level of use of the decision-making model and the agent's activity to predict the level of OSN security; the level

of consideration of the influence of the social environment; the level of consideration of subject-subject relations; the level of efficiency of the model of subject-subject relations; the level of use of the characteristics of relations for subject-subject relations; the level of use of subject-subject relations, which are derived from the human model; the level of use of types of subject-subject relations; the level of use of objective characteristics of subject-subject relations (results of joint activity); the level of adequacy in forecasting subject-subject relations in time; the level of adequacy in forecasting subject-subject relations; the level of adequacy in predicting the formation of structures in the OSN; the level of adequacy in forecasting processes in structures in OSN; the level of use of the human model in game-theoretic methods of OSN modeling.

Protection of one-level social networks from negative impact on the basis of game-theoretic solution of information security management problems. Here are a number of examples of the application of game theory to solving problems of information security management. Classical problems [4-7,31-38] will be considered as subject areas. The classification of scenarios for methods of counteracting a given threat to information security by the indicator of its economic efficiency is given in [76]

A "typical representative" is chosen as the subject of information security, which narrows the range of possible tasks to those that meet such conditions.

- All subjects of management from this class (for example, the top management of the company) are the same. That is, the individual characteristics of people are not taken into account.
- Only typical strategies are considered, which allows you to significantly reduce their number. However, this means that only typical situations that are most often encountered in the management process are considered. For information security management tasks, this means that, in all likelihood, a separate game-theoretic model needs to be built for each scenario.
- The influence of the interior is assumed to be given and fixed in order to be able to unambiguously set the utility function of the players. This means that, in all likelihood, for different aspects of the enterprise's activities, it will be necessary to build different game-theoretic models (for example, to communicate with various other subjects – for example, consumers and suppliers).

1. Let's consider the coordination of the interests of players (subjects) in the case when they are all separate people.

Example 4.1. Information security is a component of the economic potential of an enterprise [4-7,31-38]. In [48] a game-theoretic model for reducing information risk by coordinating the interests of managers (top management) of the enterprise and its shareholders is considered. In general, the interests of managers and shareholders do not coincide: shareholders are interested in increasing payments on shares, while managers are interested in increasing payments for the development of the enterprise. In order to motivate managers to increase in payments to shareholders, in [48] a scheme for the distribution of payments between shareholders and managers has been developed in such a way that it becomes advantageous for managers to make current decisions on the management of the enterprise in such a way as to increase payments to shareholders (who do not participate in the management of the enterprise).

It should be noted that here we have a typical task of information security management, and in the context of information asymmetry: shareholders have much less information about the company than managers. Of course, it is possible to force managers to "work for the payment of shares" – for example, by establishing control over them. But firstly, controllers need to be paid a lot ("for honesty"), secondly, controllers themselves must be high-level managers (in order to understand the activities of managers), and, thirdly, their presence will lead to delays in decision-making and the fear of managers to make an independent decision (for which there is no "receipt" of controllers). And this, as a result, will lead to additional economic losses of the enterprise.

Thus, the incentive method proposed in [48] allows to reduce the level of information risk for shareholders.

Example 4.2. When several enterprises (as subjects of activity) interact with each other, a situation often arises when decisions are made by specific people. This makes it possible to simulate such tasks of information protection, in which the interests of the parties – decision-makers – are coordinated.

In [71] a dynamic game-theoretic model has been built, which describes the level of protection of a social group by coordinating the interests of an official of the accumulative pension fund and an entrepreneur who is granted a loan from this fund. Although this task, at first glance, refers to ensuring the economic security of the

state, but, as the results [68] show, its solution is possible within the framework of information security management.

The model takes into account the possibility of malicious actions on the part of both an official and an entrepreneur, as well as the possibility of punishment for such actions and for inaction. The quantitative conditions for the performance indicators of officials and entrepreneurs, under which the accumulative pension system will work effectively, have been identified.

$$\begin{cases} (\alpha-\beta)S_0 - V_1 > p(S_0 - V); \\ \delta > r - w \end{cases} \tag{4.2}$$

These conditions include, for the official, the ratio (inequality) between his salary δ, the (averaged) value r of the bribes received and the cost of servicing the bribe w. For the entrepreneur, as a condition, the inequality between certain complexes is obtained, which include the rate of profit from entrepreneurial activity α, the amount of funds received from the fund S_0 and the rate of credit rate β, the cost of production (provision of services) V_1, the cost of concealing theft V and the probability p of avoiding punishment for it.

Analysis of the results of this model allowed to formulate a number of conditions for the directions of activity of the state, only after the fulfillment of which it is possible to implement the second level of pension reform.

2. Let's consider the coordination of the interests of players (subjects) in the case when one of them is an individual, and the other is an enterprise, public institution or state.

Example 4.3. The economic potential of an enterprise, a component of which is information security [4,6], includes the innovative potential of an enterprise. It should be emphasized that it is for innovations that the risks of information security are the highest. In [53,72] a dynamic game-theoretic model for the interaction of the employee and the enterprise in the interior of the enterprise's participation in innovative activities is built. The company's costs for 1) purchase of new equipment (technologies) as domestic, and in foreign markets, 2) additional payment to employees for an increased level of education, 3) income of the enterprise (taking into account the level of education of employees). For employees, only surcharges for the increased level of the world are taken into account.

As a result of solving the game, it is shown that under the assumption that the income from the use of innovative domestic or foreign equipment (technologies) is the same, the Nash equilibrium is the purchase of domestic equipment (technologies) and investment in innovative structures of Ukraine, and it is expedient to train employees (improve their skills) in Ukraine. In general, this condition can be written in the form of such an inequality.

$$(I_{in} - I_{out}) + (C_{out} - C_{in}) + (\delta_{out} - \delta_{in}) + t > 0 \tag{4.3}$$

Here, the in and out indices correspond to Ukraine and a foreign country, respectively. C – expenses for the purchase of equipment, δ – additional payment to the employee for additional education received by him/her, t – payments of the enterprise for the training of the employee abroad, I – income of the enterprise from the use of innovative equipment.

Inequality (4.3) allows for a number of measures to manage the security of the domestic economy. It should be emphasized that this inequality determines the range of information that is necessary for decision-making.

Example 4.4. Enterprise security requires informing about the benefits of using financial institutions. The risks of information security in the financial sector are always the highest, so maintaining confidentiality plays a crucial role here. Today, with the development of access to information in the world, transaction costs for access to international financial institutions have become quite small.

In [53,73] a basic game-theoretic model has been built to analyze the choice of an entrepreneur regarding the channel of investment in the development of his own enterprise. Two possibilities are considered: self-investment through the financial structures of Ukraine, and through international structures. Analysis of the model shows that investing through foreign financial institutions becomes profitable under this condition.

$$I > I_c = \frac{(1-\alpha_2)\Delta_1 + \Delta_2 + (\Delta_{iH} - \Delta_H)}{\beta - \alpha_1 - \alpha_2 + \alpha_1 \cdot \alpha_2} \tag{4.4}$$

Here, I is the investment funds that the entrepreneur wants to invest, I_c is the critical value of the investment funds, α_1 is the transaction costs in Ukraine, which

are proportional to the amount of the investment, and Δ_1 is expressed as a fixed amount α_2, and Δ_2 are the same for foreign financial institutions (and the costs of creating a foreign financial structure must be included in the fixed amount), Δ_{iH} – transfer costs in Ukraine for the transfer of the amount abroad, β – transaction losses when investing in Ukraine (e.g. "kickbacks"), Δ_H – transaction costs when investing in Ukraine, which are paid in the form of a fixed amount.

As shown by quantitative assessments made in [53], investing "abroad" for Ukrainian entrepreneurs becomes minimally profitable with amounts of more than 200 thousand rubles. euro. Thus, only sufficiently large enterprises can use such an investment channel directly. In Ukraine, the channel works extremely efficiently: the bulk of foreign direct investment, both export and import, is focused on Cyprus, where transaction costs are the lowest. [53] also identifies a number of threats to the economic security of the state.

3. Let's consider the coordination of the interests of players (subjects) in the case when they are enterprises, public institutions and states.

Example 4.5. For the case when the subjects of the game are the financial structures of a developed and undeveloped country, the risks of information security increase in comparison with the case when the financial systems of countries with the same level of development interact.

In [53] a dynamic game-theoretic model is built to coordinate the interests of the parties constructed. Two main conclusions were drawn from the analysis of this game.

The first conclusion concerns the conditions under which developed financial structures will come to undeveloped markets, in particular, in Ukraine. This condition looks like this:

$$p_U \geq \frac{p_d \cdot c_d}{c_U} \tag{4.5}$$

Here p – the probability of repayment of the loan, c – the value of the loan rate, indexes U and d denote characteristics for Ukraine and developed countries, respectively.

Estimating the ratio of credit rates in Europe and in Ukraine can be estimated as 1:5, it is possible to get an assessment $p_U \geq 0{,}2 \cdot p_d$ for (6.5). The assessment shows

that even if *all* loans are repaid to developed countries, it is profitable for foreign financial institutions to enter the Ukrainian market, even if the probability of repayment of the loan is quite small. And in the conditions of the financial crisis, when the riskiness of loans in developed countries increases (accordingly, the probability of repayment decreases), the financial structures of developed countries will enter the Ukrainian market more actively.

This situation increases the threats to Ukraine's national security due to the growing risks of instability of the financial system: foreign banks are set to export capital from Ukraine (to pay dividends to their shareholders, for example), moreover, in the event of a deterioration in the financial situation in Ukraine, they immediately curtail their work, leaving the Ukrainian economy without credit support (Ukrainian banks do not have the appropriate financial resources).

Actually, this is exactly the situation that was observed during the global financial crisis.

The second conclusion concerns the formation of domestic property prices in Ukraine, and the role of financial structures of developed countries in this.

The level of property prices can be estimated as follows.

$$C \le \frac{P}{r} \tag{4.6}$$

C – property price, P – annual income from property ownership, r – deposit rate.

The ratio (4.6) is obtained as a condition that the funds received for the property, deposited, should bring no more profit than when these funds are deposited in the bank (otherwise, the property will not be bought).

Then the i index for comparing prices for the same property in Ukraine and in developed countries can be calculated using the following formula.

$$i = \frac{C_d}{C_U} = \frac{r_U}{r_d} \cdot \frac{P_d}{P_U} \tag{4.7}$$

Indexes U and d denote characteristics for Ukraine and developed countries, respectively.

The ratio of deposit rates in Ukraine and in developed countries can be estimated as 1:10. The annual return on ownership can be estimated as $1:(1 \div 10)$: for the ownership of large *manufacturing enterprises of export* direction (metallurgical, chemical, etc.), this profit does not differ much from the profit of the corresponding foreign firms, and for small and medium-sized businesses (which are focused mainly on the domestic market) the difference will be significant. Then for the comparison index (10) we can get the following ratio.

$$\frac{C_U}{C_d} \approx 0{,}1 \div 0{,}01 \tag{4.8}$$

The correlation shows that there are quite large risks for the economic security of Ukraine at the stage of transition to a developed state. These risks lie in the fact that at the beginning of such a transition, the price of property is ten times lower, and affordable for people and structures that are not able to effectively manage it. Therefore, the massive purchase of property by foreign residents can significantly slow down the economic development. Another risk is that property can be bought up for speculative purposes: the differences in its price can be dozens of times.

Example 4.6. The methodological approach to the social network as a set of subjects of information security allows to obtain a number of new results. In [32, 33] a method for determining the time for the creation of an innovative enterprise as a factor of information security has been developed, taking into account the specifics of communications between the innovator and applicants for cooperation, which is based on the patterns of communication in a social network.

In [33] a model for determining the level of efficiency of a joint project in network Web-resources on the basis of communicative indicators was developed, which made it possible to extend the methods of sociometrics to social networks.

In [34] a model has been developed to describe the dynamics of spatial effects of the process of dissemination of public opinion within the framework of considering society as a continuous medium and its analysis. These results make it possible to apply a powerful mathematical apparatus describing a number of self-organization processes to the tasks of information and psychological security in social networks.

4.3. Method of protection of multi-level social networks

The process of protecting a multi-level social network from the negative impact of Si=MSN is shown in Fig. 4.3. Explanations in the text of the dissertation.

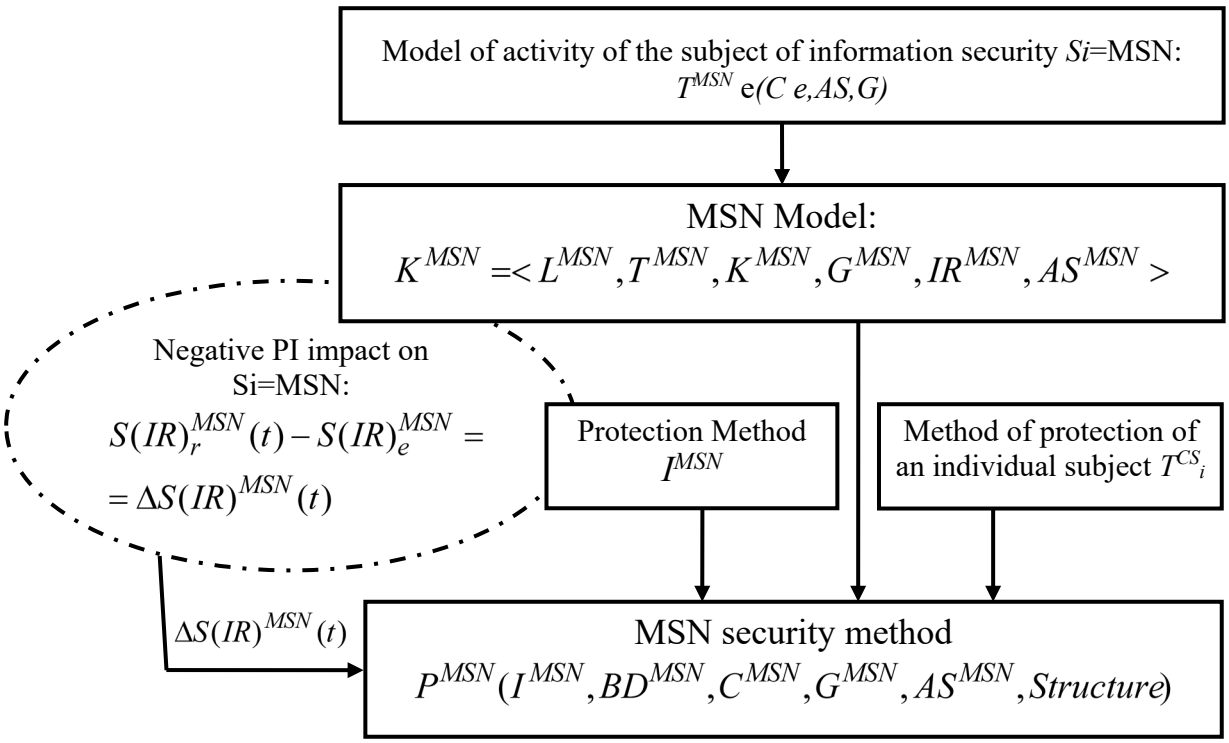

FIg. 4.3 The process of protecting a multi-level social network from the negative impact of Si=MSN

To protect a multi-level social network (MSN) from negative information and psychological influence, consider the following tuple.

$$K^{MSN} =< L^{MSN}, T^{MSN}, K^{MSN}, G^{MSN}, IR^{MSN}, AS^{MSN} > \qquad (4.9)$$

where L – a set of hierarchical levels in the MSN;

T – a set of 2AIA classes of characteristics of the activities of information security subjects – agents in MSN;

K – a multitude of coordinators in the MSN;

G – the purpose of the MSN;

IR – a set of binary relationships between agents as between 2AIA classes, including relations between coordinators and between coordinators and replicators;

AS – a set of subject areas of activity in MSN.

The method of protecting MSN from negative information and psychological influence can be presented in the following form.

Stage 1. The set of L hierarchical levels in MSN is defined. At the same time, all possible hierarchical structures of agents operating within different subject areas are taken into account. Thus, the set L consists of the numbers li(L, where and numbers the individual hierarchical structures in the MSN, and li determines the number of levels in this structure.

Stage 2. The set of T classes 2AIA of the characteristics of agents' activities in MSN is determined. Each individual subject of information security is thus defined as Simt, where i denotes a separate hierarchical structure in the MSN, m(li is the level in this hierarchical structure, and t is the class 2AIA to which this entity belongs.

Stage 3. The set K of the coordinator in the MSN is determined, taking into account their level. Thus, an individual coordinator is designated as k_{imt}.

Stage 4. Define the MSN goal and the set of goals for each level. The target of the entire MSN as a whole is denoted as $g_0 \in G$. The target for the m-th level in the i-th hierarchy is denoted as g_{im}.

Stage 5. Defined subject areas for agent activity at each level, for each level, and for MSN as a whole. Thus, the relevant subject areas are denoted as $as_{imta} \in AS$ where *i* denotes the *i-th* hierarchical structure, *m* is the level in this structure, *t* is the activity class 2AIA for the *a*-th agent at this level.

Stage 6. All existing binary relationships between agents at each level and binary relationships between agents that are at different levels are defined. Thus, the relationship between two agents in MSN is denoted as $ir_{(imt)1(imt)2}$.

Stage 7. The relationship structure of agents in MSN is compared with the relationship structure of a structured social group in Section 4.4. Structures in MSN that coincide with a hierarchically organized structured social group are identified in accordance with subsections 4.3 and 4.4. As a result, MSN can be represented as a set of hierarchically structured social groups that have a different number of levels of hierarchy and interact with each other (the highest level the hierarchy of which does not exceed, of course, the hierarchical level of MSN).

Stage 8. For each individual structured group, its protection from negative information and psychological influence is carried out according to the appropriate method.

Thus, for the protection of MSN, the following methods of protection from negative information and psychological influence, developed and improved in the dissertation, are used as scled elements:

1. Method of protection of the information space of the subject of information security $\Delta IS(t) \xrightarrow[C]{} \varnothing$. At the same time, the subjects of information security are understood as an individual, as well as a social group (unstructured and structured) and a social network (one-level);
2. Method of protection of an individual subject of information security $\Delta R(t) \xrightarrow[E]{} \varnothing$. It applies to every MSN agent (both the duplicator and the coordinator);
3. Method of protecting an unstructured social group $\Delta R(t) \xrightarrow[F]{} \varnothing$, which is applied within each of the hierarchical levels of the MSN;
4. Method of protection of a structured social group $\Delta R(t) \xrightarrow[MS]{} \varnothing$, which applies to individual hierarchical structures in MSN;
5. a method of protecting an individual subject or social group that adapts to an organized social environment $\begin{cases} \left\| \left(A_{en} + \Delta A_{en}\right) - A_{h(sg)} \right\| \xrightarrow[in]{} \min \\ \left\| \left(R_{en} + \Delta R_{en}\right) - R_{h(sg)} \right\| \xrightarrow[in]{} \min \end{cases}$, which is used for individual subjects (social groups) that are integrated into a hierarchical system of a higher level, yanage in them;
6. A method for protecting a single-level social network $Game^{OSN} =< P^{OSN}, Strat^{OSN},, U^{OSN}, R^{OSN}, Inf^{OSN} >$, which is applied within each of the individual hierarchical levels.

In addition to the above-mentioned methods of protecting subjects from negative information and psychological influence, MSN uses the ability of coordinators to actively influence the formation of appropriate hierarchical levels in MSN, to organize information at individual levels of MSN by increasing the existing set of levels and taking into account the characteristics of its individual subjects (both coordinators and replicators), using improved game-theoretic model to coordinate the interests of the parties, taking into account the information influence of coordinators on the choice of strategies for agents-replicators.

The following set of criteria has been developed to evaluate methods of protection of a multi-level social network from negative information and psychological influence: the level of justification of the model of activity of the MSN agent; the level of consideration of the negative information impact on the subject – the MSN agent; the level of completeness and sufficiency of the model of the MSN agent's activity; the level of consideration of the types of activities of agents; the level of consideration of the influence of the social environment on the MSN agent; the level of use of objective characteristics of the MSN agent's activities; the level of adequacy in predicting the decision-making and activities of the MSN agent; the level of use of the decision-making model and the agent's activities to predict the level of MSN security ; the level of consideration of the influence of the social environment; the level of consideration of subject-subject relations; the level of efficiency of the model of subject-subject relations; the level of use of the characteristics of relations for subject-subject relations; the level of use of subject-subject relations, which are derived from the human model; the level of use of types of subject-subject relations; the level of use of objective characteristics of subject-subject relations (results of joint activity); the level of adequacy in forecasting the development of subject-subject relations in time; the level of adequacy in forecasting subject-subject relations; the level of adequacy in predicting the results of MSN's activities in new conditions; the level of reliability in identifying agents-leaders , agents-talents (coordinators) in MSN; the level of adequacy in predicting the impact of agents-leaders (coordinators) on the performance of MSN; the level of adequacy in forecasting the relationship between coordinators and replicators; the level of adequacy in predicting the structuring of MSN structuring ; the level of adequacy in predicting the hierarchical structure of the MSN; the level of efficiency of using the method of describing the interaction of two or more hierarchical structures in MSN.

Thus, the results of the expert evaluation indicate that the proposed method leads to an increase in the protection of a multi-level social network from negative information and psychological influence.

Protection of multi-level social networks from negative impacts based on the set of 2AIA classes. When protecting multi-level (hierarchical) multi-agent systems from negative information and psychological influence, it is necessary to compress information when transmitting information to a higher level and detailing information when transferring it to a lower level [34].

Table 4.1. Comparison of developed and existing methods of protection of multi-level social networks from negative informational and psychological influence.

№	Characteristics of the method	Social media methods from homogeneous agents	Game-theoretic methods	Proposed method
1	2	3	4	5
1	The object of the method is a social group	+	+	+
2	The object of the method is an individual	–	–	+
3	The method is applied to a social group	–	+	+
4	The method allows you to highlight leaders and talents	–	–	+
5	Level of justification of the method: causal; statistical; heuristic (expert); Forecast and forecast verification.	 – +/– +/– –	 – + + –	 + – – +
6	A human model is required to apply the method	+	+	–
7	The method incorporates a human model	–	–	+
8	The method uses the characteristics of all people	+	+	–
9	The method uses the characteristics of an individual	–	–	+
10	Use the characteristics of the results of activitiesi	–	–	+
11	Information about a person allows you to predict: – structures in a social group; – the hierarchy of the social group	 – –	 – –	 + +

The optimality of MSN functioning is understood, firstly, as the selection of such agents who are able to adequately carry out the inter-level transformation of information and, secondly, the creation of such a network for interaction between these agents, which is adequate to their potential. Thus, an important scientific problem for the creation of optimal multi-level management systems for public institutions is the formation of an adequate model for the activities of agents, taking into account their potential capabilities to process information. The key factor in this

case is the ability to identify the agent's properties for the inter-level transformation of management information.

In [83-88] hierarchical multi-agent systems, which are modeled by acyclic graphs, are considered. Despite the results obtained, the assumption about the acyclicity of graphs is such that it significantly narrows the possibilities of applying the obtained results to the solution of applied problems. In particular, in most production and organizational structures, management teams are present at each level of the hierarchy. And this means the need to introduce cyclic graphs into consideration.

In order to build the MSNs that are used to carry out activities and manage based on the results obtained in the dissertation, it is necessary to make a number of assumptions.

Assumptions 4.1. At each of the MSN level, the management process can only be carried out with the help of agents that have a certain class of 2AIA.

This assumption holds, for example, for all organizational systems that include the human being.

The method of forming such interaction between MSN agents in order to process information and choose a solution in the most efficient way is described in the author's works [63,71,78]. This is accomplished by combining all 2AIA classes into a single structure (which we will call "socion") in a special way. A socion is a structure that consists of all 16 classes of 2AIA, provided that all possible connections between the classes of 2AIA are involved, that is, it is a cyclic graph of complex structure.

In order for MSN to exist, there must be an agent at each of its levels that is capable of communicating with lower-level agents. If there is no agent with such abilities, then the interaction between the corresponding levels of MSN cannot be carried out. Hence the following condition of optimality.

Optimality condition 1. At each level in the MSN, which has an optimal structure, at least one socion (formed from all classes of 2AIA) must function.

Definitions 4.8. An agent who belongs to a higher level in MSN and is able to communicate with lower-level agents will be called a "coordinator" (for the corresponding lower level in MSN).

Definition 4.9. An agent who belongs to a given level in MSN will be referred to as a "replicator" (or "executor" in relation to a higher level).

Optimality condition 2. At each of the levels (except the lowest) in the MSN, which has an optimal structure, there must be at least one coordinator.

This optimality condition essentially captures the need for feedback between levels in the MSN. First, the coordinator sets the task for the implementation of management for agents at a lower level, and then, having received information about the results of management, decides to achieve the goal. Fig. 4.2 takes into account that the goal of management always refers to a higher hierarchical level than the mechanisms, methods or technologies for its implementation.

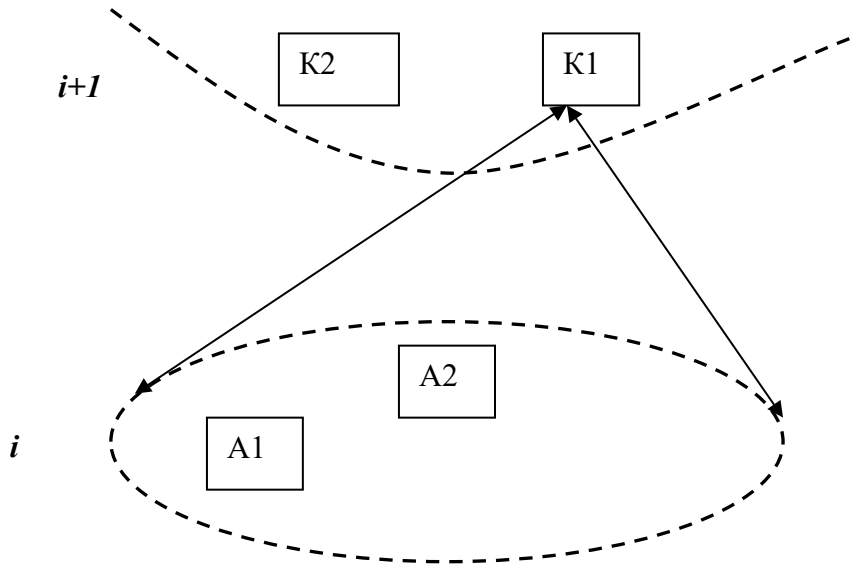

Fig. 4.4. Interaction of the coordinator with a lower level in the IMS

Let's note the specific features of the functioning of agents at higher levels in MSN. For them, there are 2 different kinds of relationships between other agents in MSN. The first type is the relationship between agents as between classes of 2AIA. They take place when management is carried out at the same level. The second type of relationship is the relationship between the coordinator and the replicator, i.e. the relationship between the 2AIA classes, that belong to adjacent levels in MSN. Note that joint activities can only be between the described agents: for example, there can be no joint management activities between agents "between whom" there is one level (due to the fact that it is impossible to fully agree on the goals of management and methods for its implementation).

Example 4.7. When constructing optimal multi-level production and organizational structures, the principle of both hierarchy and heterarchy is used.

Hierarchy means that the organizational structure is built "from top to bottom", from the coordinator of the appropriate level all the way to the employees. At the same time, only the level of coordinators (or even one coordinator) who "start"

the organization is of fundamental importance. This organization is able to "grow" only to the level that corresponds to the highest level of its coordinators.

Heterarchy means that the entire organizational structure will work optimally only if "all places" in the management pyramid are "occupied" by coordinators and replicators of the appropriate level. The absence of at least one replicator "at the very bottom" is just as critical to optimal functioning as the presence of a top-level coordinator.

Example 4.8. From the point of view of the "rarity" of agents, it should be noted that coordinators are quite rare. And the higher their level, the less common they are (that is, the smaller their number). Thus, from the point of view of the success of building an organizational structure, the most "narrow" and critical link is the involvement of the organization's management in the work.

Example 4.9. The concept of "coordinator" is defined in relation to a specific task. As a result, the organization will function effectively only until the purpose for which it was created is fulfilled. Once the goal is achieved, the organization's activities become ineffective. And the further functioning of its previous leadership poses a threat to the existence of the organization.

Example 4.10. The constructed BSMs carry out exponential compression of information (when information moves "from bottom to top") and its exponential detailing and parallelization (when information moves "from top to bottom"). This becomes possible as a result of the hierarchically organized compression of information and the parallelization of its processing at lower levels of the hierarchy. This makes it possible to use NP algorithms for control [97].

Thus, for the first time, the requirements for the organizational structure of automata capable of processing NP-algorithms are obtained.

Social structures to protect multi-level social networks from negative information and psychological influence. Information and analytical activities are one of the main elements of the information security system of the state, and national security in general [32-34]. With the development of the global telecommunications network Internet, in which today there is simply a huge number of documents, it becomes, oddly enough, more and more difficult to consolidate information. Moreover, today it is becoming increasingly clear that cyberspace can serve as a powerful amplifier of information influence, and this amplification is exponential. Events in North Africa and many countries around the world are case in point.

Thus, the task of reforming the structures of information and analytical activities in state and public structures, the task of reforming the very system of carrying out such activities, is an urgent scientific and important practical task.

There are fundamental books on information security of the state [4-7], which set out the main technologies for analysis and decision-making in the subject area of information security of the state. However, the description of the formation and functioning of information and analytical structures in public and state institutions in these fundamental sources is not given the necessary attention. "By default" they believe that such information and analytical structures are in the right quantity and that they function optimally.

A model for describing the effective interaction of state structures and the media both in the period before possible emergencies and in emergency situations is given in [91].

The analytical services of each state rely on a set of experts. Expert scientists play a particularly important role: they are the ones who develop new methods, mechanisms and technologies of information and analytical activities. For the information security of the state, the most important is played by those scientists who work in the humanitarian sphere, primarily in the socio-economic sphere. It is within this subject area that new methods for objectification and modeling of socio-economic processes are developed, and it is in this subject area that the verification of the developed proposals is carried out.

For example, Ukraine is at the stage of reforming powerful and effective analytical structures. The scientific potential of the country still needs measures to improve, as evidenced by the results of comparing the activities of domestic scientists with foreign ones [4, 7-23].

In addition, in some higher education institutions there is a situation of so-called "adverse selection" [49], in which not the best graduates are involved in postgraduate studies and teaching.

4.4. Conclusion to Chapter 4

1. A model of an unstructured social group, where agents belong to certain classes of 2AIA characteristics of the activities of information security subjects, has been proposed. It is shown that such social networks can refer to a finite set of classes that differ in topological characteristics, these characteristics arise as a result of

taking into account closed paths in the social network, which arise due to the presence of asymmetric relations.

2. Improved game-theoretic models for matching the interests of agents in an unstructured social network, where agents belong to certain classes of 2AIA characteristics of the activities of information security subjects. The specific characteristics of such games, which are introduced by the agent's belonging to the appropriate class 2AIA, have been revealed.

3. The method of protection of one-level social networks from negative information and psychological influence has been improved, which differs from the proposed method for the protection of an unstructured social group in that it uses specially defined subsets of network agents, which are formed with the use of asymmetric binary operators of relations between agents, as well as improved theoretical-game models of coordination of agents' interests, which allowed to ensure adequate representation and structuring information to differentiate agent access, as well as protection against attacks on individual agents.

4. An additional consideration of the ability of coordinators to influence the formation of appropriate hierarchical levels in a multi-level social network is proposed. This ensures the ordering of information at individual levels of a multi-level social network by increasing the existing set of levels and taking into account the characteristics of its individual subjects (both coordinators and replicators). An improved game-theoretic model for harmonizing the interests of the parties, taking into account the information the influence of coordinators on the choice of strategies for replicating agents.

5. The method of protection of multi-level social networks from negative information and psychological influence has been improved, which differs from the proposed method for the protection of a structured social group in that it expands the ability of coordinators to influence the formation of appropriate hierarchical levels in a multi-level social network, ensures the ordering of information at individual levels of a multi-level social network by increasing the existing set of levels and taking into account the characteristics of its individual subjects (both coordinators and replicators), uses an improved game-theoretic model to coordinate the interests of the parties, taking into account the information influence of coordinators on the choice of strategies for agents-replicators, which made it possible to take into account additional factors to ensure the protection of a multi-level social network from negative influence and to link the level of the agent (coordinator) with the required level of its protection from third-party information influence.

Conclusions

1. The National Security Strategy of Ukraine, the Military Doctrine of Ukraine, the Cybersecurity Strategy of Ukraine and other documents emphasize the growing need to strengthen measures to protect a person and a social group from negative information and informational-psychological influence, the need to develop new methods and means for the implementation of these activities. The standards of the ISO/IEC 27000 – 27037 Information technology – Security techniques series set the requirements for the development, operation and modernization of information security management systems (ISMS), which also includes the need to model the activities of information security subjects. It has been found that today violations of information security by the subjects of information security in the world are massive. It is shown that the informational-psychological factors used in the process of building models of protection of a person and a social group as subjects of information protection originate from management, psychology, sociology and game theory. Which is clearly insufficient, since it cannot be integrated into information security models.

2. It is shown that in modern models of description of information security processes, the subject component (a person or a social group) is modeled at the level of implementation of the given formal rules, and these rules relate to both interaction with the objects of information protection and interaction between subjects. It is shown that there is a need to develop such models of activity of subjects and subject-subject interaction, which allow to carry out formal modeling.

3. The existing models of management of subjects, which originate from psychology, sociology and management, are analyzed. It is shown that for the tasks of information and psychological security there is a need to develop new models of human activity and human interaction, since the existing models cannot be effectively used.

4. The proposed tool is a promising tool for identifying agents ofconfidentiality threats in the case when agents are part of a social network. Grouping of quantitative values of coefficients $R_{\leftarrow}$, $R_{\rightarrow}$ and M_i allows you to analyze information processes in the social network, to identify informal agents of influence on the network and agents that are ignored by the network, and those agents who actually ignore the activities of the network (almost without taking part in its activities).

5. The proposed remedy is used without the participation of agents of the social network, which excludes the distortion of the results of the study, since the channel of uncontrolled influence on the social network is excluded. This increases the level of reliability of the data obtained. The proposed computer program is a powerful tool for monitoring social networks, as it can be used even in the background. This allows you to get the dynamics of the coefficients $R_{\leftarrow}$, $R_{\rightarrow}$ and M_i in its temporal unfolding. In particular, it allows you to detect agents who become a potential privacy threat in time.

6. The paper is the first to develop a model for constructing an information space for a given subject of information security, which is based on the specifics of perception and processing of information, features of decision-making and implementation of activities of the subject of information security, which led to the division of an integral database into eight subsets using three dichotomous operators.

7. The paper describes the method of using the information space of the subject of information security to protect subjects from attacks on the components of the information space, to identify the presence of such influence and its specific characteristics, as well as to counteract the negative information and psychological impact on the formation of an adequate goal of the information space.

8. For the first time, a methodology for comprehensive protection of a person and structured and unstructured social groups has been developed, taking into account the possibility of adaptation of individual subjects in need of protection and their groups to the organized social environment, as well as one- and multi-level social networks from negative information and psychological influence, which takes into account the classes of characteristics of the activity of an individual subject and a finite set of classes of binary relations between these subjects using certain operators, which made it possible to ensure the protection of various kinds of subjects and subject groups from negative information and psychological influence.

9. For the first time, the model of structuring the information space of the activities of individual subjects of information security is used to apply in the development of a method of protecting the subject from information and psychological influence. It is proved that arbitrary activity in the information space can be described by two-component operators, which translate one component of the information space, which describes the subject area of activity before the implementation of the activity, into one component of another information space, which describes the subject area of activity after the implementation of the activity.

It is proved that in order to describe arbitrary activity in the subject area of the task, it is necessary, in general, to have 64 two-component operators that translate the information space "before the activity" into the information space "after the activity". It is shown that simple regulators and systems of positive and negative feedback can be described as certain such operators.

10. A method of protecting a person from negative information and psychological influence isproposed, which uses the proposed model of structuring the information space of individual subjects to protect against influence, as well as dividing the set of characteristics of activity into subsets with characteristics characteristic of a wide range of subjects and an individual subject, allocating the characteristics of the subject's activity from 16 defined classes (classes are distinguished by the poles of dichotomies "participant – observer", "generalizing – detailing" and others), which made it possible to identify factors, channels and characteristics.

Referens

1. Challenges and threats to critical infrastructure. NGO Institute for Cyberspace Research (Detroit, Michigan, USA), 2023. 325 p.

2. Melzer N. The Trial of Julian Assange: A Story of Persecution. London : Verso Books, 2022. 368 p.

3. Ozhiganova M. I. Personnel management / M. I. Ozhiganova, V. O. Khoroshko, Yu. E. Yaremchuk, V. V. Karpinets. Vinnytsia: VNTU, 2014. 188 p. *(in Ukraine)*

4. Andreev V. I. Information security management strategy / V. I. Andreev, V. D. Kozyura, L. M. Skachek, V. O. Khoroshko. K.: DUIKT, 2007. 277 p. *(in Ukraine)*

5. Bogush V. M. Information security of the state / V. M. Bogush, O. K. Yudin. K.: "MK-Press", 2005. 432 p. *(in Ukraine)*

6. Andreev V. I. Fundamentals of information security / V. I. Andreev, V. O. Khoroshko, V. S. Cherednychenko, M. E. Shelest. K.: Ed. DUIKT, 2009. 292 p. *(in Ukraine)*

7. Bogush V. M. Theoretical foundations of protected information technologies / V. M. Bogush, O. A. Dovydkov, V. G. Kryvutsa. K.: DUIKT, 2010. 454 p. *(in Ukraine)*

8. Moroz O.V., Nikiforova L.O., Shiyan A.A. Socio-psychological factors of motivating employees of instrument-making enterprises. Vinnytsia: VNTU, 2011. 252 p. *(in Ukraine)*

9. Kokun O.M. Psychophysiology. Tutorial. K: Center for Educational Literature, 2006. 184 p. *(in Ukraine)*

10. Makarchuk M. Yu., Kutsenko T. V., Kravchenko V. I., Danilov S. A. Psychophysiology. K.: "Interservice" LLC, 2011. 329 p. (in Ukraine)

11. Kuziv O.E. Psychophysiology. Ternopil: branch of TNTU named after I. Pulyuya, 2017. 194 p. *(in Ukraine)*

12 Dilts R. B. Changing Belief Systems With NLP. Dilts Strategy Group, 2018. 236 p.

13. Bandler, R., Grinder, J. (1981), Reframing: Neuro-Linguistic Programming and the Transformation of Meaning, Real People Press, 1982. 208 p.

14. Piattelli-Palmarini M. Inevitable Illusions: How Mistakes of Reason Rule Our Minds / M. Piattelli-Palmarini. New York : Wiley, 1996. 256 p.

15. Fundamentals of social psychology / Gornostay P. P., Slyusarevskyi M. M., Tatenko V. O., Tytarenko T. M., Khazratova N. V. and others. ; under the editorship M. M. Slyusarevskyi. Kyiv: Talkom, 2018. 580 p. *(in Ukraine)*

16. Social psychology: teaching. manual for bachelor's degree holders / N. Yu. Volyanyuk, G. V. Lozhkin, O. V. Vynoslavska, I. O. Blokhina, M. O. Kononets, O. V. Moskalenko, O. I. Bokovets, B. V Andriytsev; KPI named after Igor Sikorsky. Kyiv: KPI named after Igor Sikorskyi, 2019. 254 p. *(in Ukraine)*

17. Moskalenko V.V. Social Psychology. K.: Center of Educational Literature, 2008. 688 p. *(in Ukraine)*

18. Kozlova O.A. Social psychology of personality and communication Kharkiv: NTU "KhPI", 2017. 172 p. *(in Ukraine)*

19. Hjelle L. A., Ziegler D. Personality Theories: Basic Assumptions, Research and Applications. McGraw-Hill Publishing Co., 1992. 624 p.

20. Nashinets-Naumova A. Yu. Information security: the issue of legal regulation. K: Helvetica, 2017. 286 p.

21. Kataev E. S. Information and psychological security of the individual in the conditions of modern society. Bulletin of the National Defense University of Ukraine. 2014. 2 (39). P. 215-220. *(in Ukraine)*

22. Cialdini R.B. Influence: The Psychology of Persuasion. Harper Business, 2006. 336 p.

23. Kuleba D. War for reality. How to win in the world of fakes, truths and communities. #knygolav, 2022. 384 p. *(in Ukraine)*

24. Pomerantsev P. This is not propaganda. A journey to war against reality. Yakaboo Publishing, 2020. 288. *(in Ukraine)*

25. Forward S., Frazier D. Emotional Blackmail: When the People in Your Life Use Fear, Obligation, and Guilt to Manipulate You. Harper Paperbacks, 2019. 272 p.

26. Psychology of personality: Bibliography / O. B. Melnychuk, R. F. Pasichnyak, L. M. Volnova, etc. K.: NPU named after M.P. Dragomanov, 2009. 532 p. *(in Ukraine)*

27. Stolyarenko O. B. Personality Psychology. K.: Center of educational literature, 2012. 280 p. *(in Ukraine)*

28. Moskalets V. P. Personality Psychology. Kyiv: Lira-K Publishing House, 2020. 364 p. *(in Ukraine)*

29. Le Bon G. Psychology of Crowds. Sparkling Books, 2009. 224 p.

30. Katsavets R.S. Personality psychology. Tutorial. Kyiv: Alerta. 2021. 134 p. *(in Ukraine)*

31. Understanding strategic adaptations: security strategies and policies after 2014. Eds. H. Maksak, R. Q. Turcsanyi and M. Vorotnyuk. Bratislava, Kyiv, 2018. 167 p.

32. Mattis J. N. (Lieutenant General), Hoffman F. (Lieutenant Colonel). Future Warfare: The Rise of Hybrid Wars. Proceedings Magazine (US Naval Institute). 2005. V.132/11/1,233.

33. Shifting Paradigm of War: Hybrid Warfare. Eds. Yücel Özel, Ertan Inaltekin. İstanbul, National Defense University, 2017. 116 p.

34. Kurban O.V. Modern information wars in the online network space. Kyiv: VIKNU, 2016. 286 p. *(in Ukraine)*

35. Kulyavets V.O. Forecasting of socio-economic processes. K.: Condor, 2009. 194 p. *(in Ukraine)*

36. Voytovych R.V. The impact of globalization on the system of public administration (theoretical and methodological analysis): Monograph / General. ed. Dr. Philos. Sciences, Prof. V.M. Knyazeva. K.: Publishing House of NADU, 2007. 680 p. *(in Ukraine)*

37. Social technologies: for what? how? with what result? / Sciences. ed. V. I. Podshivalkina. Odesa: Odesa National University named after I. Mechnikov, 2014. 546 p. *(in Ukraine)*

38. Grebenyuk A. M., Rybalchenko L. V. Fundamentals of information security management. Dnipro: Dniprop. state inside of affairs, 2020. 144 p. *(in Ukraine)*

39. Shiyan A.A., Abramchuk I.V., Humenyuk V.V. Peculiarities of managing the moral and ethical state of the population during the war in the information space. Materials of the VI International Scientific and Practical Conference "Information Security and Computer Technologies": abstracts of reports, April 20-21, 2023. Kropyvnytskyi: National Technical University, 2023. P.91. *(in Ukraine)*

40. Azarova A. O., Bilichenko N. O., Mironova Yu. V., Tkachuk L. M. Methodology and organization of scientific research. Vinnytsia: VNTU, 2022. (PDF, 117 p.) *(in Ukraine)*

41.Sheldrake J. . Management theory : from Taylorism to Japanization. London : International Thomson Business Press, 1996. 225 p.

42.Schelling T.C. The strategy of conflict. Harvard University Press, 1981. 328 p.

43.Zlepko S. M. Information technologies for managing human activity / S. M. Zlepko, A. A. Shyian, S. V. Pavlov, I. I. Haimzon. Vinnytsia: VNTU, 2012. 316 p. *(in Ukraine)*

44.Jacob L. Moreno Sociometry, Experimental Method and the Science of Society. Lulu.com, 2012. 238 p.

45.Niyati Aggrawal, Adarsh Anand. Social Networks Modelling and Analysis. CRC Press, 2022. 236 p.

46.Easley D. Networks, Crowds, and Markets: Reasoning about a Highly Connected World / D. Easley, J. Kleinberg. Cambridge : Cambridge University Press, 2010. – 833 p.

47.Jackson M. O. Social and Economic Networks / M. O. Jackson. Princeton : Princeton University Press, 2010. 520 p.

48.Shyian A. A. Management of development of socio-economic systems. Game theory: basics and applications in economics and management / A. A. Shiyan. Vinnytsia: VNTU, 2010. 162 p. *(in Ukraine)*

49.Mas-Collel A. Microeconomic Theory / A. Mas-Collel, M. D. Whinston, J. R. Green. Oxford: Oxford University Press, 1995. 977 p.

50.Gibbons R. Game Theory for Applied Economists / R. Gibbons. Princeton: Princeton University Press, 1992. 288 p.

51.Sandler T. The analytical study of terrorism: Taking stock / T. Sandler // Journal of Peace Research. 2014. V. 51, N. 2. P. 257-271.

52.Sandler T. An Economic Perspective on Transnational Terrorism / T. Sandler, W. Enders // European Journal of Political Economy. 2004. N.20(2). P. 301-316.

53. Shyian A. A. Management of the formation of effective economic institutions for Ukraine / A. A. Shiyan, L. O. Nikiforova. Vinnytsia: VNTU, 2011. 300 p. *(in Ukraine)*

54. Nikiforova, L. O. Mechanism of interaction of financial institutions: Arrow-Debre economy / L. O. Nikiforova, A. A. Shyian // Proceedings of the VII International Scientific and Practical Conference "Research and Optimization of Economic Processes "Optimum – 2010"" (December 1-3, 2010) Kharkiv, 2010. P. 34. *(in Ukraine)*

55. Coupé T. The visibility of Ukrainian economists 1969–2005 / T. Coupé // Journal of Socio-Economics. – 2008. – V.37. – P.2114-2125.

56. Maslow A. H. Motivation and personality. Longman, 1987. 336 p.

57. Rogers C. R., On Becoming A Person: A Therapist's View of Psychotherapy. Mariner Books, 2012. 444 p.

58. Kast F. E. Organization and management: A systems approach. McGraw-Hill, 1974. 655 p.

59. Gruber T. R. A Translation Approach to Portable Ontologies / T. R. Gruber // Knowledge Acquisition. 1993. V.5(2). P.199-220.

60. Gruber T. R. Toward Principles for the Design of Ontologies Used for Knowledge Sharing / T. R. Gruber // International Journal of Human Computer Studies. 1995. V.43(5-6). P.907-928.

61. Handbook on Ontologies / eds. S. Staab and R. Studer. – International Handbooks on Information Systems, Berlin : Springer, 2009. – 832 p.

62. Noy N. F. Ontology Development 101: A Guide to Creating Your First Ontology / N. F. Noy, D. L. McGuinness. – Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001. 25 p. http://protege.stanford.edu/publications/ontology_development/ontology101.html .

63. Guarino N. What Is an Ontology? / N. Guarino, D. Oberle, S. Staab / In S. Staab and R. Studer (eds.). // Handbook on Ontologies. International Handbooks on Information Systems, Berlin : Springer, 2009. P. 1-20.

64. Shiyan A. A. Types of Economic Behavior: The Instrument for Management of Individuals, Institutions, Countries and Humankind / A. A. Shiyan, L. O. Nikiforova // Information Systems: Behavioral & Social Methods eJournal. 2011. V. 3, Issue 161, November 15. 22 p. Available at SSRN: http://ssrn.com/abstract=1952651.

65. Buryachok V. L. The possibility of providing protection against informational and psychological influence based on the universal method of building

ontologies / V. L. Buryachok, A. A. Shyian // Modern information protection. 2013. No. 4. P. 57-67. *(in Ukraine)*

66. Shiyan A. A. The construction of a structure for Information Space for control problems in industrial and organizational structures / A. A. Shiyan // Materiały VIII międzynarodowej naukowi-praktycznej konferencji «Aktualne problemy nowoczesnych nauk – 2012» 07-15 czerwca 2012 roku. Volume 47: Techniczne nauki. Przemyśl : Nauka i studia, 2012. P. 54-57.

67. Dirac P. A. M. The Principles of Quantum Mechanics. Clarendon Press Publication, 1982. 324 p.

68. Feynman R. P. Statistical Mechanics: A Set of Lectures. CRC Press, 1998. 372 p.

69. Feynman R. P. The Character of Physical Law: The 1964 Messenger Lectures. Cambridge : THE M.I.T. PRESS, 1985. 173 p.

70. Feynman R. P. Elementary Particles and the Laws of Physics: The 1986 Dirac Memorial Lectures. Cambridge : Cambridge University Press, 1987. 60 p.

71. Shyian A. A. Game-theoretic analysis of rational human behavior and decision-making in the management of socio-economic systems / A. A. Shyian. Vinnytsia: UNIVERSUM-Vinnytsia, 2009. 404 p. *(in Ukraine)*

72. Shyian A. A. Methods of using game-theoretic models of economic processes to coordinate the interests of the parties / A. A. Shyian, N. S. Parpolita // Materials for the 6th international scientific and practical conference "Latest achievements in European science 2010". Sofia: "Byal GRAD-BG" OOD, 2010. Volume 5: Economies. P.79-81. *(in Ukraine)*

73. Shyian A. A. Information space and classification of strategies of managerial activity in the theory of games and decision-making / A. A. Shyian // Information technologies and computer engineering. 2007. No. 3(10). P. 131-139. *(in Ukraine)*

74. Shyian A. A. Conceptual problems of human description: self-organization of life against the background of energy and substance flows – from cell to mind / A. A. Shyian // Optical-electronic information-energy technologies. 2003. 1-2(5-6). P. 177-184. *(in Ukraine)*

75. Buryachok V. L., Shyian A. A. Classification of technologies for the implementation of information and psychological influence on the process of rational human activity // Modern protection of information. 2014. No. 1. P. 64-70. *(in Ukraine)*

76. Buryachok, V. L. Peculiarities of designing protection systems against the negative consequences of informational and psychological influence / V. L. Buryachok, A. A. Shyian // Modern special technology. 2013. No. 4. P. 92-98. *(in Ukraine)*

77. Shyian A. A. Methodology of complex protection of people and social groups from negative informational and psychological influence / A. A. Shyian // Security of information. 2016.T1. P. 45-51. *(in Ukraine)*

78. Shyian A. A. Technologies for HR-Managers: Typology for Person's Economic Behavior, Applications and Mechanism Design / A. A. Shyian // Labor: Personnel Economics eJournal. 2011. V. 3, Issue 70. 373 p. Available at SSRN: http://ssrn.com/abstract=1827706.

79. Shyian A. A. Classification of the meaningful component of the analyst's world picture / A. A. Shyian, V. V. Karpinets // International conference "Knowledge management and competitive intelligence". Kharkiv, Khnure, 2013. P. 165-166. *(in Ukraine)*

80. Shyian A. A. Hierarchical ontologies for automation of management of organizational structures / A. A. Shyian // Bulletin of the National University "Lviv Polytechnic". Thermal power engineering. Environmental engineering. Automation. 2014. No. 792. P. 32-36. *(in Ukraine)*

81. Yaremchuk Yu. E. Approach to the formation of hierarchical classifications of methods of protection of telecommunication networks from negative influence / Yu. E. Yaremchuk, A. A. Shiyan // Measuring and computing equipment in technological processes. 2014. No. 4. P. 226-230. *(in Ukraine)*

82. Shyian A. A. The method of modeling the activity of information security subjects using operators operating in the ontologies of subject areas / A. A. Shiyan // Informatics and mathematical methods in modeling. 2013. Vol. 3, No. 4. P. 342-352. *(in Ukraine)*

83. Shyian A.A. Modeling of activity in the class of ontologies of subject areas loaded with a goal / A. A. Shyian // Modeling and computer graphics: Materials of the 5th international scientific and technical conference, Donetsk, September 24-27, 2013 – Donetsk, DonNTU, Ministry of Education and Science of Ukraine, 2013. P. 12-26. *(in Ukraine)*

84. Shiyan A. A. Operators in the information space for the problem of control in industrial and organizational systems / A. A. Shiyan // Materialy VIII mezinarodni vědecko – prakticka konference «Aktualni vymoženosti vědy – 2012». 27 června – 05 červenců 2012 roku. Dil 22. Technickй vědy. Tělovychova a sport: Praha. Publishing House «Education and Science» s.r.o., 2012. P. 47-50.

85. Howard A. Elementary Linear Algebra. New York : Wiley, 1987. 475 p.

86. Dekel E. Topologies on Types / E. Dekel, D. Fudenberg, S. Morris // Theoretical Economics. 2006. V. 1. P. 275-309.

87. Dekel E,. Interim Rationalizability / E. Dekel, D. Fudenberg, S. Morris // Theoretical Economics. 2007. V. 2. P. 15-40.

88. Bloch E. D. A First Course in Geometric Topology and Differential Geometry. Boston : Birkhäuser Boston, MA, 1997. 421 p.

89. Shyian, A. A. Model of creation of automated technological process control systems using mathematical operators in the information space / A. A. Shyian, Yu. Ye. Yaremchuk, L. O. Nikiforova, V. Kh. Kasiyanenko // Measurement and calculation technology in technological processes. 2015. No. 1. P. 236-239. *(in Ukraine)*

90. Dorf R. C., Bishop H. Modern Control Systems. New York: Prentice Hall, 2010. 1104 p.

91. Levi M. The Mathematical Mechanic: Using Physical Reasoning to Solve Problems. Princeton: Princeton University Press, 200 p.

92. Shyian A. A. Economic cybernetics: introduction to modeling of social and economic systems / A. A. Shiyan. – Lviv: "Magnolia 2006", 2007. 228 p. *(in Ukraine)*

93. Roik O. M. System analysis. / O. M. Roik, A. A. Shyian, L. O. Nikiforova. VNTU, 2013. 131 p. *(in Ukraine)*

94. Nebava, M. I. Theory and training in management decision-making technology / M. I. Nebava, A. A. Shyian. Vinnytsia: VNTU, 2009. 59 p. *(in Ukraine)*

95. Shyian A. A. Management of material and technical supply in crisis conditions / A. A. Shyian, L. L. Karpovych, L. O. Nikiforova // Materialy V Miedzynarodowej naukowi-practicznej konferencji "Wyksztalcene I nauka bez granic – 1009". Przemysl: Nauka I studia, 2009. – Vol. 5: Economiczne nauki. P. 28-30. *(in Ukraine)*

96. Shyian A. A. Mechanism and technologies for team management based on the model of deterministic finite automata / A. A. Shiyan, L. O. Nikiforova, T. K. Meshcheryakova // Bulletin of the Khmelnytskyi National University. Economic sciences. 2012. N 2., T. 1. P. 46-49. *(in Ukraine)*

97. Hopcroft, John E., Motwani R., Ullman J.D. Introduction to Automata Theory, Languages, and Computation. Boston: Pearson Education, 2007. 550 p.

98. Shyian A. A. Social and psychological portraits of politicians: O. O. Moroz, N. M. Vitrenko and V. P. Horbulin / A. A. Shyian // Nova Politika. 1998. No. 4. P. 24-28. *(in Ukraine)*

99. Shyian A. A. About the role of communicators in ensuring psychological comfort: from stress to suicide / A. A. Shyian // Applied psychology. 2000. No. 4. P. 67-79. *(in Ukraine)*

100. Shyian A. A. About methods of persuasion in politics: the use of interpersonal relations / A. A. Shyian // Political marketing. 2000. No. 8. P. 28-46. *(in Ukraine)*

101. Shyian A. A. Elections in Ukraine: a technological impasse / A. A. Shyian // Political marketing. 2006. No. 5. P. 31-38. *(in Ukraine)*

102. Medinska B. G. Mathematical modeling of SPPR elements for effective work with customers / B. G. Medinska, A. A. Shyian, L. O. Nikiforova // Collection of scientific papers of the IV International Scientific and Practical Conference "Alliance of Sciences: Scientist – to a scientist" (Dnipropetrovsk, March 18-19, 2009). Volume 1. P. 82-84. *(in Ukraine)*

103. Shyian, A. A. Technological approach to learning in IT specialties / A. A. Shyian // Proceedings of the 8th International Scientific and Practical Conference "Internet – Education – Science (ION-2012)". Vinnytsia, 2012. P. 107-108. *(in Ukraine)*

104. Belzetskyi R. S. The method of identification of physiological characteristics of the emotional status of soldiers of special units of the Ministry of Internal Affairs depending on their types of activity / R. S. Belzetskyi, A. A. Shyian // Bulletin of the Vinnytsia Polytechnic Institute. 2013. Issue 6. P. 8-10. *(in Ukraine)*

105. Belzetskyi R. S. Use of feedback in the management of a special unit / R. S. Belzetskyi, A. A. Shyian // Proceedings of the 5th International Scientific and Practical Conference "Modern Problems of Radio Electronics, Telecommunications and Instrumentation (SPRTP-2011). Vinnytsia, May 19-21, 2011. Vinnytsia: VNTU, 2011. P. 149-150. *(in Ukraine)*

106. Malhotra N. K. Marketing Research: An Applied Orientation. Pearson, 2009. 897 p.

107. Ryan P. Y. A. Mathematical Models of Computer Security. Lecture Notes in Computer Science 2171, Springer 2001, pp. 1-62.

108. Korniyenk B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. Information Security. 2017. V. 34, No. 2. P. 114-118.

109. Bisikalo, O. V., Kovtun, V. V., Yukhimchuk, M. S. (). MODELING THE SECURITY POLICY OF THE INFORMATION SYSTEM FOR CRITICAL USE. Radio Electronics, Computer Science, Control. 2019. No 1. P. 132-149.

110. Banks M. J. On Confidentiality and Formal Methods. Submitted for the degree of Doctor of Philosophy. The University of York. Department of Computer Science. March 2012. 256 p. https://www.cs.york.ac.uk/plasma/publications/pdf/BanksThesis.12.pdf.

111. Bell, D. E., LaPadula, L. J. Secure Computer Systems: Mathematical Foundations. MITRE CORP BEDFORD MA, 1973. 42 p. https://apps.dtic.mil/sti/pdfs/AD0770768.pdf.

112. Shyian A. A., Nikiforova L. O. The method of calculating the effectiveness of people's joint economic activity based on game-theoretic modeling / A.A. Shyian, L.O. Nikiforova // Bulletin of the National Technical University "Khpy". 2008. No. 54(2). P. 10-13. *(in Ukraine)*

113. Shyian A. A. The practical recommendations of manager for determination of dual among the subordinates / A. A. Shyian, L. O. Nikiforova, V. O. Krulov / Materialy v Mezinárodni vêdecko-practická konference "Efectivni nászété modernich vêd – 2009". 27.04 – 05.05.2009. Dil. 3. Economic kê vêdy. Praha: Publishing House "Education and Science", 2009. P. 22-24. *(in Ukraine)*

114. Shyian A. A. Mathematical modeling of the joint economic activity of people / A. A. Shyian // Scientific works of VNTU. 2008. No. 2. 7 p. *(in Ukraine)*

Шиян, А. А.

Ш65 Забезпечення інформаційної безпеки та кібербезпеки в сучасному інформаційному просторі: моделі та методи : монографія (англ. мовою) [Електронний ресурс] / А. А. Шиян, Л. О. Нікіфорова. – Вінниця: ВНТУ, 2024. – (PDF, 135 с.).

ISBN 978-617-8163-02-0 (PDF)

У монографії обґрунтовано необхідність протидії загрозам кібербезпеки; наведено аналіз сучасних моделей і методів управління інформаційною безпекою; представлено розроблений ефективний метод виявлення агентів загроз у задачах кібербезпеки та метод побудови інформаційного простору суб'єктів інформаційної безпеки тощо. Монографія призначена для науковців, аспірантів і магістрів та широкого кола фахівців з кібербезпеки.

УДК 331.101.3

ISBN 978-617-8163-02-0 (PDF)

Електронне наукове видання

Шиян Анатолій Антонович
Нікіфорова Лілія Олександрівна

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ: МОДЕЛІ ТА МЕТОДИ

Англійською мовою

Монографія

Рукопис оформила *Л. Нікіфорова*

Оригінал-макет підготовлено *в редакційно-видавничому відділі ВНТУ*

Підписано до видання 15.02.2024.
Гарнітура Times New Roman.
Зам. № Р2024-048.

Видавець та виготовлювач
Вінницький національний технічний університет,
Редакційно-видавничий відділ.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95, м. Вінниця, 21021.
press.vntu.edu.ua;
Email: irvc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.