The Ministry of Education of the Republic of Belarus
Educational Establishment
“The Belarusian State University
of Informatics and Radioelectronics”

UDK 004.056

Abdulhadi
Hasn Abubakr Hasn

Methods of Assessment of Social and Psychological Influence on Population for Information Security Systems

ABSTRACT

for the degree of Master of Science in Engineering
in specialty 1-98 80 01 “ Information Protection Methods and Systems and Information Security

Scientific adviser
Leonid Mikhailovich Lynkov
Doctor of Science in Engineering and
Professor

GENERAL CHARACTERISTICS OF THE WORK

Information means of disorganization of society are based on ideas of social and psychological influence. This theory is spread by controlled influence on household, social and political, energy, military strategic and other components of state life support.
This influence includes means of process and transmission of information, mass media, transnational corporations, political and religious organizations and special services. Social and psychological influence is characterized by the principle of continuity of ideology and technology for control of the world or local social and political situation.
This work provides review of up-to-date methods and means of controlled influence on the state population and proposes methods and techniques to reduce social and political information hazards and threads.
The topicality of the work is in the necessity to reduce the level of influence of negative information factors on the state population by counteraction to threads of this influence and organization of state and public control and resource support. It is shown that the results of information influence mostly manifest in cases of crisis.
The scientific novelty is in the development of methods of assessment of social and psychological influence and methods of forecast of most probable situations, as well as determination of functions and preventive arrangements.
The practical value is in reveal of possible ways of social and psychological influence on population by means of process and transmission of information and development of a complex of recommendations to reduce the effect of this influence by resource support.
Defended provisions:
1. It is shown that social and psychological influence is one of most significant factors of neurolinguistic programming of the population for disorganization of the society, which leads to low level of control in cases of emergency (accidents, disasters, military and social conflicts).
2. A system of protection of the population against subthreshold information by monitoring of control of foreign and domestic threads, public sentiments and possible correction via multimedia systems is proposed.
The results of the dissertation have been published in 3 printed works (2 theses and 1 article in materials of the international conference .

INTRODUCTION

Currently, information and psychological security is the main strategic object of complex influence made in form of secret operations of information and psychological warfare that determines the nature of choice of purposes and objectives, formation and use of forces and means of secret operations at various levels: the operational one, the tactical one and the strategic one. Information and psychological security is one of priority directions of national security of countries. It is worth mentioning that systems of social relations of the modern information society make quite strong influence on its formation and development, which lets consider this system an environment of organization and realization of information and psychological influence. Moreover, use of social and psychological means and methods is one of main tools of unauthorized access to information .

1-THE METHODOLOGY OF INFORMATION AND PSYCHOLOGICAL SECURITY

1.1. The role and place of information and psychological security in the modern society

In modern conditions, information warfare is an effective but not used to the full extent means of provision of geopolitical balance. Solution of practical tasks of geopolitical competitive warfare using means and methods of information warfare lets, in particular, even weak countries and coalitions preserve relative independence in form of choice of their own foreign policy and ability to appropriately (asymmetrically) response to challenges of competing geopolitical entities. As the information and telecommunications network infrastructure develops, even districts most distant from the line of immediate contact with probable opponents and objects located there become within the area of reach of up-to-date destruction means. The geopolitical space acquires new dimensions, comprising the information and information and psychological space .

The technological evolution becomes a source of principally new threats, offering earlier unavailable opportunities of negative influence on person, society and state. The information sphere turns into a backbone factor of life of people, societies and states. There increases the role and impact of mass media and global communication mechanisms on the economic, political and social situation. Information technologies have found wide use in control of most important objects of life support that become increasingly vulnerable to accidental and intentional influence. Evolution of information warfare as a new independent strategic form of global competition is observed. The practice of targeted information pressure is spread that significantly affects national interests.

National interests are a combination of needs of the state for realization of balanced interests of person, society and state securing constitutional rights, freedom, high living standard of citizens, independence, territorial integrity, sovereignty and sustainable development.

In the social sphere, the main national interests include:

- satisfaction of main social needs of the citizens, minimization of negative effects of social differentiation and social tenseness;
- provision of public security and security of life of population, as well as reduction of the level of crime and criminalization of the society;
- provision of employment of citizens and appropriate level of remuneration;
- development of intellectual, as well as religious and moral potential of the society, preserving and augmenting its cultural heritage, as well as strengthening the public spirit;
- provision of harmonious development of international and interconfessional relations.

The main national interests in the information sphere include:

- realization of constitutional rights of the citizens for receipt, storage and distribution of comprehensive, true and timely information;
- formation and steady development of the information society;
- equal participation in world information relations;
- transformation of the information industry into an export-oriented economy sector;
- effective information support of the state policy;
- provision of reliable and sustainable functioning of critical informatization objects.

It is worth mentioning that an important information and psychological feature of expansion of participants of geopolitical competition is information (information and psychological) neocolonialism dividing all states and regions of the world into entities dominating in the information and psychological space and being the sources of expansion and entities lacking

the required information resources, technologies and developed information and telecommunications infrastructure and thus being informationally dependent on the dominant entities .

A special role in the information and psychological warfare of mass information and mass communication media, transnational information and telecommunications corporations and virtual social (network) communities requires careful study of effects of engagement of these information space entities in information confrontation on part of various participant of the conflict.

1.2. Classification of threats of information and psychological influence on society and methods to resist their realization

The source of threat to the national security is a factor or combination of factors that can under certain conditions lead to emergence of threat to national security [4].

The main potential or actually existing threats to the national security include:

- infringement of independence, territorial integrity, sovereignty and constitutional system;
- forcing policy not meeting its national interests, interference from outside in domestic processes;
- insufficient competitiveness of the economy;
- decrease of welfare and the living standard of the population;
- destabilization of the national financial and monetary and credit system, as well as loss of stability of the national currency;
- incapability to return and serve foreign and domestic debt;
- impossibility of guaranteed provision of raw materials and energy resources in the volumes assuring the targeted growth of the gross domestic product;
- loss of foreign markets, including as a result of discrimination of Belarusian manufacturers;
- lag in the rate of transition of the economy to advanced technological systems of other states, degradation of the structure of the real sector of the economy;
- depopulation, general ageing of the nation, decrease of the birth rate, deterioration of other main figures of the national demography health;
- increase of criminal and other illegal infringements against person and property, manifestations of corruption;
- preparation or realization of terroristic acts in the territory or airspace, use of the territory or airspace by terroristic organizations and groups against other states;
- manifestations of social and political, religious, ethical extremism and racial hatred in the territory;
- unrest accompanied by violence or threat of violence on part of a group of persons or organizations resulting in emergence of danger to life and health of persons, independence, territorial integrity, sovereignty and existence of state;
- disorganization of the state management system, creation of obstructions in functioning of the public institutions;
- activation of emigration processes, growth of uncontrolled immigration in the state;
- instability of the social security system;
- increase of unemployment, including unregistered and hidden one;
- destructive information influence on person, society and public institutions affecting the national interests;
- distortion of functioning of critical informatization objects;

- emergence in the territory or close to its borders of large-scale natural or technogenic cases of emergency, epidemics and epizooty;
- insufficient volumes and poor quality of foreign investments;
- decrease of the scientific and technological, as well as educational potential to the level not assuring innovation development;
- illegal distribution or traffic across the territory of weapons of mass destruction, their components and delivery means, dual-purpose technologies and equipment, weapons, ammunition, radioactive, chemical and other dangerous substances and materials;
- loss by a significant part of the citizens of traditional values and guides, attempts of destruction of national religious and moral traditions and biased reconsideration of history affecting these values or traditions;
- sharp or large-scale decrease of trust of the citizens to main public institutions;
- targeted infringement of life, health and freedom of citizens staying abroad;
- insufficient scale and level of introduction of advanced information and communication technologies;
- decrease or loss of competitiveness of domestic information and communication technologies, information resources and the national content;
- degradation of land, forests and natural complexes, exhaustion of mineral raw materials, water and biological resources;
- radioactive, chemical and biological pollution of soil, land, water, subsoil, plants and atmosphere;
- loss or disclosure of information constituting secret protected by laws or capable of affecting the national security.

In the social sphere, domestic sources of threats to the national security include:
- sharp social stratification and high differentiation of income of the population;
- insufficient motivation of employees for effective labor and economic activity, distribution of sentiment of social dependency;
- unjustified disproportion in the sphere of remuneration and pension fund;
- professional qualification and territorial unbalance of demand and offer of labor, low domestic mobility of the population;
- significant differences in the living standards of urban and rural population, citizens of big, medium and small cities;
- decrease of the number of working population;
- non-provision of a part of the population with affordable housing of due quality, unsolved housing problems of the citizens;
- insufficient organization and technological level of development of the social sphere;
- lag of the quality of education by a number of perspective directions from the level of world best educational centers, insufficient number of advanced high-qualification specialists of the world level;
- increase of epidemic diseases, increase of the number of persons suffering from socially dangerous illnesses and increase of the number of the disabled;
- change of the system of life values of the young generation in the direction of weakening of patriotism and traditional moral values;
- criminal tendencies and manifestation in the society;
- low security culture of life of the population;
- functioning of sects and pseudo-religious groups.

In the information sphere, domestic sources of threats to the national security include:
- spread of untrue or intentionally misleading information affecting the national interests;

- dependence on import of information technologies, means of informatization and protection of information, their uncontrolled use in systems failure or destruction of that can affect the national security;
- incompliance of the national content with the world level;
- insufficient development of the state system of management of the process of implementing and use of information technologies;
- increase of crime using of information and communication technologies;
- insufficient efficiency of information support of the state policy;
- imperfect system of security of critical informatization objects.

It is worth mentioning that in the general case the threat structure is a complex of the threat object, threat source and threat manifestation, so for a more detailed classification of threats the following characteristics may be used:

– the location of the threat source;
– probability of realization and expected damage;
– the source type;
– the security object type.

Perfecting the state policy in the sphere of international and interconfessional relations will be in provision of conditions for strengthening of uniform community, cultivation of respect to other nationalities, religions and cultures, exclusion of any attempts to incite national and religious hatred.

An important role in assurance of security in the social sphere is to be played by programs of employment of the population, secondary and vocational education, prevention and treatment of socially relevant diseases, prevention of crime (first of all, among minors), housing construction, preservation of the historical and cultural heritage and so on .

Protection against foreign threats to the national security in the information sphere is to be performed by participation in international treaties regulating in view of equality world information exchange, in creation and use of interstate and international global information networks and systems. For exclusion of technological dependence, the state retains the role of the regulator by introduction of foreign information technologies.

1.3. Types of information and psychological influence in social systems

Currently, widely used there become forces, means and methods of information and psychological influence (including forces, means and methods of information and psychological warfare as the most dangerous and aggressive manifestation of this influence) as the main tool to get geopolitical dominance.

Term “psychological warfare” in its not strictly scientific (common) sense characterizes the following:

- political activity of certain persons, groups, parties and movements;
- election campaigns of candidates for various election positions;
- advertising activity of commercial companies;
- warfare of competing individuals (as well as minor groups) for leadership in production, scientific and other collectives;
- political, economic or cultural confrontation of conflicting ethnoses;
- negotiation between competing companies or organizations.

The psychological warfare includes organization and realization of various psychological operations and events aimed at:

- distortion of information received by the administration of the competitor (opponent) and suggestion to them of false and meaningless information that prevents them from correct understanding of events or the current situation and making correct decisions;
- brainwashing of social groups (the entire popularity);
- ideological sabotage and misinformation;
- maintenance of positive public opinion;
- organization of mass demonstrations under false slogans;
- propaganda and spreading of false rumors.

Considering of psychological warfare in its wide sense as a purposeful and systematic use by political opponents of propaganda and other means (diplomatic, military, economic, political, etc.) for direct or indirect influence on opinions, sentiments, feelings and thus behavior of the opponent to make them act as it is desirable for the other party we can say that being an element of the system of political relations, psychological warfare is present in various dimensions of this system not only as the foreign policy but also as the domestic one. The complex strategy of information and psychological influence on the attacked object described above is illustrated by Figure 1.1.

The complex strategy of influence

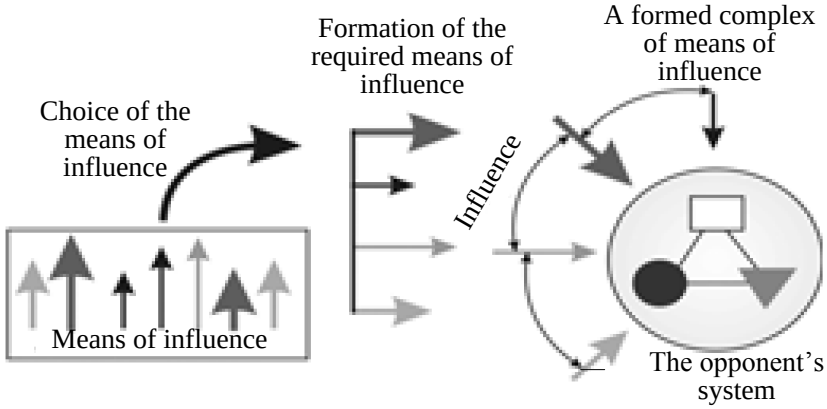


Figure 1.1 – Complex strategy of information and psychological influence on the attacked object

Figure 1.2 shows the information process as a way to influence the population.

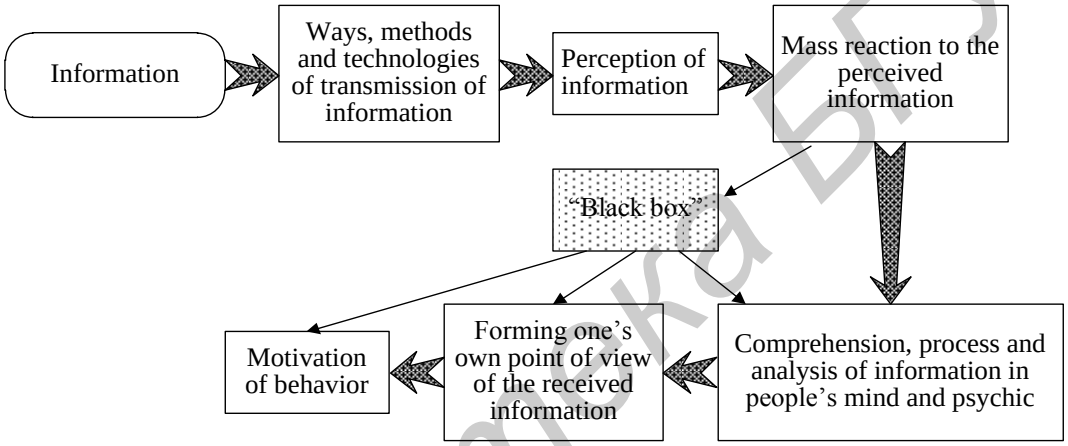


Figure 1.2 –The information process as a way to influence the population

Strict classification of these elements of information and psychological influence is very difficult, since fragments of information and psychological operations and events observed by analysis of diplomatic actions, various propaganda, PR and election campaigns strike imagination with diverse forms of techniques and technologies used in them. Mere listing of these elements with reference to actual conditions or situations (the operational state) within that they were realized is inexpedient.

2- MAIN REQUIREMENTS FOR INFORMATION SYSTEMS OF GOVERNMENT AUTHORITIES

2.1. CREATION OF INFORMATION SYSTEMS OF GOVERNMENT

Information systems of government authorities are to provide:
- assured and safe access to public government information resources;
- possibility to search for, collect, process and store state information resources;
- possibility to provide government authorities access to local and global information resources;
- reliability of operation and tolerance to software and hardware faults, including cases of incorrect user operation;
- operational and safe exchange of data between users;
- possibility of further expansion by upgrade of hardware and software, addition of new system components;
- other functions related to the main activity of the government authorities.

Information systems of government authorities include:
- information and analytical systems ensuring collection, process, storage and analysis of data about results of realization by government bodies of their main tasks and functions;
- electronic document flow systems;
- systems of management of electronic archives of documents;
- operation management systems (including systems of management of the infrastructure components);
- transactional and accounting systems that support realization by government authorities of their main tasks and functions;
- systems of interdepartmental information exchange between information systems of government authorities;
- resource management systems that support business processes and administrative regulations in activity of government authorities;
- systems of interaction with natural and legal persons supporting provision by government bodies via the Internet or other communication channels reference information and services, including portals and call centers;
- information security systems;
- office systems used by employees of government bodies in their daily activity for preparation of documents and exchange of information.

Creation of information systems of government authorities includes the following steps:
1) development of the requirements;
2) development of the concept;
3) statement of work, sketch and technical design, preparation of working documentation, commissioning and support.

The content of work at each stage and distribution of responsibilities of participants of creation of the information system are determined by the relevant standards.
Information systems of government authorities are to be protected in accordance with special requirements, as well as requirements of other regulatory documents. Information security in information systems of government authorities is to be provided by the system including a complex of organizational and technical measures and software and hardware protection of

information. Organizational measures are to include the list of actions and requirements regulating engagement of natural and legal persons in design, development, operation and support of information systems of government authorities .

Software and hardware means of information protection used in information systems of government authorities are to provide:

- identification of protected information resources;
- authentication of the user of the information system;
- authenticated data exchange;
- data integrity by development, transfer, use, processing and storage of information;
- authorized access to all system resources in normal operating conditions;
- differentiation of access of users to the information system resources;
- administration (determination of rights of access to the information system resources, process of information from logs, installation and removal of security system);
- registration of users' entries and exits, as well as violations of rights of access to the information system resources;
- control of integrity and operability of the information security system;
- security and uninterrupted operation of the system in cases of emergency.

The security system of information systems of government authorities is to be realized by appropriate security policy based on the National Security Concept and other regulations and ensure timely identification of security threats, as well as causes and conditions related to violation of their normal functioning .

At the same time, the current situation in the field of information systems urgently requires development of recommendations for improving the security system use of that will allow organizing development and operation of information systems of better quality and efficiency.

Experts predict that the main type of weapon of the XXI century will be high-precision weapon. It is the precision of target destruction that solves not only strategic but also political objectives of warfare. The USA offer a way out: to use a weapon that does not destroy but only wound and demoralize the opponent.

This weapon implies means of influencing people and equipment based on chemical, biological and other principles that make the opponent unfit for combat for some time and let control the situation and behavior of people managing situations so that lethal means are not used. These means include all systems of influence below the level dangerous for life: non-lethal, not that lethal, conditionally lethal. In general, term "non-lethal weapon" (NLW) applies to systems that are not intended for full destruction or substantial harm. Publications define NLW as "a weapon designed to put out of operation personnel, arms, materials and technical equipment in such a way that death or disability are unlikely".

Accordingly, NLW systems also are to have high mobility, require no significant investments or organizational measures regarding logistics and not impede decision-making.

Some NLW systems, especially high-tech ones, haven't been fully tested in real combat conditions. Some of them may be banned. For example, use of chemical agents is to take into account the relevant treaties on chemical weapons.

The effect of use of NLW is to be reversible (it doesn't always apply to NLW influencing technical equipment). The optimal non-lethal weapon is the one for that reversibility is determined only by the time factor. Some types of non-lethal weapons require use of special means, such as medicine or other forms of rehabilitation .

The purpose of need to develop non-lethal weapons influencing manpower with various functionalities is formed. These weapons are to put out of operation only those who they are aimed at, without affecting the persons who are around.

Non-lethal weapons influencing material equipment limit the opponent's possibility to use technical equipment and arms.

Currently, several types of special influence on computers of the opponent are distinguished:

- early inclusion in software of systems of weapons, management and connection of the relevant elements (they are activated upon expiration of a certain period of time, by a special signal or otherwise) that bring the serviced computers out of operation. In this case the failure looks as a natural equipment failure;
- introduction using agents, communication channels or other means of computer viruses that destroy information in databases and software of combat systems;
- entry into channels of communication between computers and introduction of false information there;
- bringing computers out of operation and erasing information using powerful microwave radiation, electromagnetic pulse or otherwise;
- speech synthesis to be used for propaganda

2.2.Development of the method of assessment of social and psychological influence on people

Security planning. Any measures of maintenance of the required level of security start with the security planning stage. Fig. 2.2 presents the security planning stage structure.

1. Understanding of priority tasks of social and psychological security
2. Forecast of most probable situations
2.1. Creation of the state governance system
2.2. Creation of the normative documents
2.3. Technical support
3. Selection and explanation of ways to assure security
3.1. Monitoring of foreign threats for the state
3.2. Monitoring of social and psychological sentiments in the state
3.3. Monitoring in the sphere of discrediting the state government
4. Definition of functions and arrangements to prevent social and psychological influence
5. Allocation and distribution of security resources
5.1. Resources for monitoring
5.2. Resources for training
5.3. Resources of power structures
5.4. Scientific support
5.5. Training the population
6. Working coordination and interaction issues at the planning stage

Fig.2.2 Proposed structure of methods of planning social and psychological security

In accordance with the proposed structure of methods of planning social and psychological security, it is to be guided as follows:
– development of the main means of security of specific processes is to be carried out taking into account the existing understanding of factors of accidents, incidents, diseases, as well as money provided for their prevention;
– by defining the security functions and the measures one is to be guided by the hierarchical multilevel structure of the relevant system and the possibility of redistribution of the solved tasks between its main components: man and machine; the main idea of this redistribution is continuous specification of their functions depending on the developed conditions;
– early distribution of security resources between the life cycle stages of the existing or developed process is to occupy a special place by formation of the program of functioning of the relevant corresponding;
– by processing interaction issues when planning the security of the developed processes, the purposes and the quantitative indexes of the relevant system are to match the purposes and indexes of the higher of the interacting system, and the required documents are to be coordinated.
Management of social and psychological security consists of a number of substages (steps):
– specification of the main tasks and the means of operational control;
– collection and process of information about real cases at production sites, in the society, etc.;
– evaluation of the need and ways of alternative influence on social and psychological processes in the society;

– selection of the complex of most effective influence;
– planning, organization and control of their realization.

Control and preventive work to prevent accidents and mass diseases is in fact the part of operational control of the security process that is realized in the course of serial production (creation and transmission of information).

Let us recall that according to this understanding, emergence of accidents by realization of processes is a result of uncontrolled output of energy and a consequence of emergence of the causal chain of prerequisites conditioned by failures of technical equipment, errors of people and off-design foreign influence.

Consequently, to maintain the required security, high quality and mutual compatibility of each of the listed components of the concerned system are to be continuously provided .

The main principles of security maintenance are to be aimed not only at prevention of accidents and diseases, but at taking measures to decrease the damage in case of their emergence, too.

3.DEVELOPMENT OF THE MAIN DIRECTIONS to reduce the INFORMATION DANGER

3.1.Development of methods of protection from subthreshold information

Methods of protection against negative sides of multimedia systems can be divided into administrative and legislative, psychological and technical.

As technical measures of security, there can be applied means and devices of detection of negative influence made by television and radio broadcasting systems. Thereby, when this negative influence is made using relatively explicit methods, in some cases signs of this negative influence can be detected by certain parameters of the signal indicating, in particular, presence in them of infralow frequencies, as well as parameters corresponding to increased emotionality. For the audio signal such parameters include change of the voice pitch, its melodic structure, timbre and aspiration; volume drops; signal rhythm at large intervals; energy spectrum in various frequency bands .

In case it is difficult to detect signs of negative influence on the part of, for instance, television and radio broadcasting systems directly by the signal, it is required to use man as a sensor of such negative influence. For this, subjective states of man can be controlled using such objective methods as the method of Voll, polygraph, the method of Kirlian, by biorhythms of the brain, etc.

At detection of negative information influence, there can be further taken information protection measures. Among them, there can be proposed:

- production of a warning signal about the dangerous nature of further stay by the TV-set;
- automatic switch off;
- automatic introduction of compensating information in form of a calming or exciting color background and calming or exciting music background;
- compensating processing of the signal to mitigate its negative influence.

Currently, quite a large number of means of presentation of video and audio information for subconscious perception has been developed, that, without knowing special codes, are so far practically undetectable using technical methods. It is surprising that the brain still extracts this information at the subconscious level and reacts to it adequately.

The more educated the man is, the more difficult it is to suggest him or her ideas conflicting his or her world view. But good education doesn't mean good, cautious mind. That's why ideas and thoughts suggested bypassing consciousness or at a changed state of consciousness become a kind of person's own. As a result, such suggestion becomes supereffective.

Man has several levels of protection the main of that is consciousness. That's why not every man is fit for subthreshold influence. Firstly, the number of channels is limited: vision and hearing. Secondly, the wish of the person him- or herself to participate in receipt of the information is essential. Finally, the cleverer the person is, more complicated the person's inner world is and more firm his or her basic moral principles are, the more difficult it is to influence and control the person. The number of people relatively easily influenced using subthreshold methods is not more than 30%, but in case such influence is against the background of deliberately induced emotional excitement, the number of people encoded this way considerably increases.

Taking into account this new type of danger, currently, psychical influence through television and radio broadcasting channels and ability to adequately react to this kind of psychical influence are important. There exist psychotherapeutic methods of work with subconsciousness not excluding consciousness from the working process. These methods let release man from various information and psychical dependencies.

Such a strategy can, for example, consist of self-coding when a person through his or her consciousness programs his or her subconsciousness to adequately react to information of subthreshold nature. Such self-coding contributes to automatic setting of a barrier between the viewer and information received from the screen and differentiates between them. Such differentiation is sufficient protection, as to neutralize the deep influence of advertisement, the slightest degree of distrust in it is enough .

Several techniques of protection influencing the mode of perception of subthreshold information are proposed:

– training immunity to the information flow;
– training critical attitude to the information flow;
– training detection of techniques of manipulation of information flows;
– abstracting from the information flow;
– detection of techniques of emotional perception the information flow.

According to the expert opinion, one of the most rational methods of blocking NLP is use of counter-NLP, i.e. reprogramming of behavior to eliminate the violent influence. Thereby, there emerge two possibilities: removal of the performed NLP and preliminary protection against the influence, in case the direction of the violent programmed behavior is known or forecast. Consequently, the task of protection against violent programming of behavior is narrowed to development of the defensive reprogramming. An important part in exit from NLP is played by the actual situation, mainly social, against that defensive reprogramming takes place. The more the patterns of the defensive reprogramming correspond to actual processes, the closer they are to the real “life truth”, the easier this reprogramming is

Several techniques of protection against the violent neurolinguistic programming are proposed:

– evaluation of the methods and detection of most vulnerable points;
– detection and search for a more powerful method of defensive neurolinguistic programming;
– designing the structure of neurolinguistic programming;
– realization of the defensive programming.

Psychological measures of security in relation to VR include increase of mental activity and caution of the users; these are so much demanded the more virtual reality goes beyond imitating traditional forms of relations mastering special forms of influence .

However, apart from self-protection and psychological protection methods, there are required services to continuously check broadcasts in television and radio broadcasting for presence of the negative aggressive information, psychophysiological influences of unconscious subthreshold suggestions and creation of VR with the right to stop any broadcast and impose sanctions.

3.2.Development of requirements for mass warning systems

Life of the modern society is impossible without mass warning about oncoming natural disasters, major transport and industrial accidents, unpredictable actions of maniacs and, at last, military threats .

Historically, for warning of population during wars and natural disasters there were used various means: smoke of fires, toll, locomotive whistles (factory whistles), etc. The need for mass warning of population of a country, region, city, city district or microdistrict is determined by the relevant events and, thus, the warning objectives.

Formulated requirements to mass warning systems are as follows:

maximal coverage of the population in the relevant territory, regardless of location of each person (at home, in a shelter, in the street, travelling by transport);

maximal warning reliability, viability of the warning system regardless of possible interruptions of power supply, communications, condition of the addressees (stress, mass panic, etc.) and external conditions (wind, flood, earthquake, explosions, etc.) preventing reception of sound information;

in each certain case the warning territory is to be located to reduce unnecessary disturbance of population in safe territories;

continuous operability (the time to make the warning system ready for transmission of a message is not to exceed several minutes for the entire warning territory);

delay in transmission of messages is not to exceed reasonable limits for all groups of the population;

there are to be taken all measures required to prevent unauthorized starting of the system, and at the same time as soon as the system is started it is not to spontaneously stop by damage of its elements;

operation of the warning system is not to interfere with operation of other life systems of the population (transport, communications or uninterrupted technological processes).

Warning systems are most mass systems , so, special attention is to be paid to their cost, convenience and servicing expenses.

In favorable circumstances, mass warning systems are never to be used. This postulate explains the difficulty of control of their life and determines their desirable integration in other mass information systems. Most compliant with the requirements for organization of mass broadcast are SB systems. Use of sound broadcast systems has changed from plain radio announcement or transmission of special signals to transmission of code signals triggering certain technical devices of mass warning, such as street sound systems or sound sirens. An up-to-date warning system is a complex of technical means using all types of communication and transmission of mass information combined with special organizational and technical arrangements in the standby and active operation mode.

The adopted concept of mass warning. Warning of the population starts with production of loud sound signals heard in the entire warning territory preceeding the voice message (information) specifying the type and place of danger, as well as ways of its minimization. Loud sound signals are produced by remotely controlled sirens combined into local (technological and object) and city or regional systems. Electromechanical sirens are in detail described in handbooks on acoustics and have been and are used most widely. The generator and emitter of sound in these sirens is rotated by electric motor powered 1.5—4.5 kVA. Start of electromechanical sirens is controlled well via the city telephone communications systems.

The main disadvantage of these sirens is complexity of provision of assured power supply due to branching of the siren network because of limited sound pressure created by each siren (110—120 dB). There are two ways to improve the siren warning system:

- increase of the sound pressure enabling to reduce by an order of magnitude the number of sirens and, consequently, provide autonomous sources of power supply and simplify the control system;
- sharp increase of the number of sirens of smaller sound capacity simplifying their structure and enabling to use electrochemical power sources (dry batteries) as a guaranteed source of power supply. The network of control of these batteries becomes rather branched and awkward.

In European states, there are produced and used so called pneumatic sirens operating from an autonomous compressor driven by the diesel or petrol motor. Airflow modulation is performed by its passage through holes in rotating discs. The sound pressure level of such sirens exceeds 140 dB, and the frequency is 2-4 kHz by power of the petrol motor of 60-80 h.p. The sound head with loudspeakers creating the required (not necessary circular in the horizontal plane) directional pattern is placed at high (100 m and more) towers.

Improvement of the element base has allowed starting production of plain small-scale electromechanical announcers quite widely used at object warning networks.

Upon production of an alarm all systems of mass information are started: radio and wired sound broadcasting, television, telephone communications and cable television systems. For transmission of alarms to bomb-proof shelters, to blockages, in addition to regular site systems, transmission of signals using wired supply networks is possible, as well as using electric fields of spreading throughout land.

Apart from increase of volume and legibility, such process reduces energy consumption of amplifiers, which is important in cases of emergency. To save the power and increase the viability of the wired broadcasting network, it is recommended to install power sharing feeders between amplifiers assuring the network operability by failure or deenergization of a part of amplifiers.

By choice of the preferable system of transmission of information for mass warning most important is the ability of subscriber devices to remain operable by deenergization of houses: the ability of passive receipt without additional conversion and amplifying of the signal. This ability is provided by wired broadcasting networks, theoretically cable television networks, telephone networks and communications system based on power supply networks.

Building the mass warning system based on telephone networks is technically tempting, as full telephonization of the region lets cheapen the entire broadcasting system. Building this system is worked in the framework of implementation of 6-program sound broadcasting via subscriber telephone networks realized in Russia.

Integration of sound broadcasting in systems of cable television is difficult, but there is hope that the process will become faster and come along with implementation of interactive (bilateral) systems, integral information systems providing for the subscribers all kinds of communications and broadcasting services and letting collect information from all subscribers of the network, practically from all residential and service rooms.

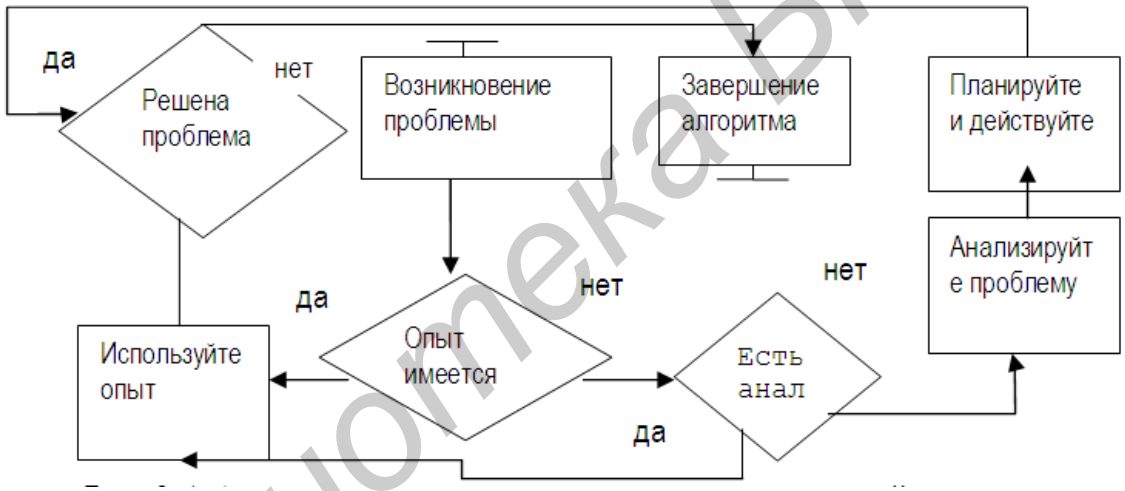
Sound warning systems are installed at practically all transport: road, rail, air, river and sea. Each bus, train, plane or ship is equipped by a wired sound broadcasting system (sound system) used mainly for technological purposes. Operation of the local warning system on transport is inseparable from technology. The main messages are generated by the driver, aircraft commander or ship captain. As transport is equipped by radio broadcasting receivers, all the passengers are covered by the general system of mass warning.

Generation of messages for mass warning systems is specific and rather responsible. Deciding on important announcements is very difficult, requires high civil courage and professional

understanding of the situation that is often beyond any instruction. The most dramatic example is the criminal delay of announcement of the actual danger during the Chernobyl disaster that led to tens of thousands of human victims. Nothing contributes to panic more than lack of timely and true information by the population.

3.3.Training people safe behavior in view of psychophysiological characteristics

As has been mentioned, behavior of man in stressful situations is impossible to forecast, which is fraught as for man himself or herself so for the environment .
Training people safe behavior is aimed to prevent accidents due to more comprehensive consideration of the human factor. The purpose of training in the psychophysiological sense is in change of behavior of people and at the extreme development of new or adjustment of already existing reflects to extreme situations connected with emergence of prerequisites for accidents.
The actual possibility of training people safe behavior is determined by that unlike that of animals human actions are not always instinctive and often need intellectual training requiring certain consumption of psychic energy and time. In normal (standard) conditions unconscious, automatic actions of people are optimal, but in case unfamiliar rare situations emerge in the consciousness there is often engaged intellectual programming for determination of the purpose, the plan of actions and the technologies of its implementation.
The algorithm of natural behavior of people in extreme situations when there are no ready decisions illustrating the above is shown on the logical diagram provided in Fig. 3.4



Да	Yes
Нет	No
Решена проблема	Problem solved
Возникновение проблемы	Problem emerged
Завершение алгоритма	Algorithm completed
Планируйте и действуйте	Plan and act
Анализируйте проблему	Analyze the problem
Используйте опыт	Use the experience
Опыт имеется	Experience available
Есть анал	There is anal

Fig. 3.4. The algorithm of human behavior in extreme situations

It is known that people trained safe behavior in time lose the obtained knowledge and skills, in particular, when they are not vital for them. This feature of people is most vividly

demonstrated by absence of accidents forming for people the so called “security system”. Thus, there emerges the task to determine the regularity of training people safe behavior. In this case it is to be considered the exponential nature of probability of error-free and timely actions of man and the exponential nature of change of psychological characteristics of man in time (reduction of the amount of information held by man after its receipt).

CONCLUSION

As a result of the conducted surveys, the main technical and social, as well as economic requirements for social and psychological security of the population are analyzed and main features of the methodology to assure it are developed. The necessity of formation of secured information systems based on the principles of reliability, confidentiality, openness and scalability is shown.

Using analysis of manners and means of assurance of information security of governmental authorities, the need of study of information processes as ways to influence the population is revealed. There are provided the main types and technologies of information and psychological influence, crisis management processes, types and manners of manipulating. The concept of use of non-lethal weapons, incl. information weapons, in regional conflicts is depicted. It is shown that use of means of influence on systems of process and transmission of the opponent's data, as well as acoustic and electromagnetic influences are capable of disabling electronic equipment and human resources, which, in its turn, calls to develop the methods and means of resistance and create security systems.

The principles of energy and information influence on individuals and groups are described, in particular, mobile telephony is considered as an element of possible change of human psychic through masking speech communications and possible encoded suggestion using various audio media.

It is shown that extreme situations are one of most important factors of neurolinguistic programming of the population for disorganization of the society, which leads to low level of control in cases of emergency (accidents, disasters, as well as military and social conflicts). Methods of planning of assurance of social and psychological security to protect the population against subthreshold information by control of its physiological condition and possible adjustment in various ways are proposed.