UDC 001.8

Methodical and Applied Aspects of Creation and Application of Cyber Ranges

Yuriy Danyk[1]

[1] *Ivan Chernyakhovsky National Defense University of Ukraine*

Abstract

The methodical and applied aspects of the creation and application of cyber ranges are proposed in the article. The new solutions for analysis, synthesis and the development of applied scientific and technological principles of construction and realization of cyber ranges are given.
These cyber ranges can be used for: research issues of cyber monitoring, cyber defense and cyber influence; design of fundamental and applied bases of constructing mathematical support of software and hardware assets for realization of monitoring processes, analytical information processing, forecasting, planning and implementation of passive and active countermeasures against information and cyber threats in cyber space. This makes it possible to check the effectiveness of new and innovative forms and methods of countermeasures against challenges and threats of terrorism, of protecting critical infrastructures, society, authorities, and person through the realization of complexes of information security in cyber space.

Keywords: cyber challenges and threats; cyber defence; cyber security; cyber space; cyber range; hybrid threats; national cyber defence system; a system of cyber threats early detection

Introduction

Nowadays combat and other actions (economic, political, energy, information and cyber) in modern military conflicts known as the hybrid warfare are correlated in idea (concept) and objectives [1].

Discussions of hybrid warfare have often centred on definitional debates over the precise nature of the term, and whether hybrid covers what other military experts describe as nonlinear warfare, full-spectrum warfare, fourth-generation warfare, or other terms [2, 3]. Similarly, discussions of cyber conflict have treated the phenomenon as a separate domain, as if using cyber tools remained distinct from other forms of conflict [4, 5]. A hybrid war that is de jure being conducted on the territory of Ukraine, and de facto encompassing more participants all over the world, in terms of its content, forms and methods of conducting- can be considered a specific variant of fourth-generation wars (4GW).

Analysis of recent research and publications. Formulation of the problem

In hybrid conflicts of any intensity, hostilities (operations) are an element of other (non-force) actions mutually coordinated according to a single plan, mainly economic, political, diplomatic, informational, psychological, cyber, cognitive, etc. This creates destabilizing internal and external processes in the state that is the object of aggression (concern and discontent of the population, migration, acts of civil disobedience, etc.). Hybrid wars are not declared and, therefore, cannot be completed in the classical sense of the end of wars and military conflicts. This is a kind of permanent war of variable intensity across multiple sectors, with cascading impacts and synergistic destructive manifestations, in which the entire population of the country and the international community are to a certain extent consciously or unconsciously involved. The impacts are felt on all spheres of life, on all sectors of society and throughout the state. Thanks to the use of innovative technologies, it became possible to shift conflict from predominantly overt and forceful (kinetic) means, to less obvious strategies focused on the structural vulnerabilities of adversaries, including (importantly) achieving a cognitive advantage over them.

The intensive development of innovative technologies has resulted in new highly technological vulnerabilities in all spheres of life activities of the countries [6]. These effects make it possible to take control and dominate over the basic institutions of the country, as well as to succeed in actualizing their interests through the unconventional and cognitive effects and mostly asymmetric actions.

Cyberspace proved the main theatre of asymmetric actions [7, 8]. It is promoted by the fact that cyberspace has an extraterritorial, universal and global character; it is also ill-adapted to national geographic borders, can serve as socializing surrounding for people of nearly all ages and is constantly expanding. The nature of cyberspace makes it possible for its users to be mobile and act anonymously, and for the source of the message (electronic resource) to be reserved or coded. Communication through cyberspace becomes almost momentary. The information flows can be realized through both the dialogue was a mass audience and the possibility of ultimately individual communication. For the time being cyberspace proves to be the most important instrument

of shaping the collective and individual consciousness and the system of values [9]. Along with it the impact itself can be efficient, creative, consolidating and at the same time destructive [10].

The analysis of numerous references makes it possible to ascertain that well-known approaches to detecting hybrid effects and vulnerabilities in cyberspace can be focused on the somewhat reduced understanding of their nature [11, 12, 13, 14].

In reality, one can observe the totality of diversified effects through cyberspace [15, 16]. The above results in the formation of target-oriented effects for realizing the goal of the entire complex of measures aimed at implementing hybrid threats. Along with it, the ultimate goal can be realized only on the basis of complementarity and interaction, as well as on the basis of the synergy of all planned measures with respect to their cause and effect relationships. Cyberspace is used for conducting psychological operations and computer network operations etc. [17].

Along with it, it is not a force impact on the enemy, but the information, cybernetic and psychological impacts that prove the basic means of realizing the objective. These effects are focused on disabling the enemy, promoting the prearranged narratives, controlling the cognitive sphere on the emotional, moral, cultural and mental levels; forming the system of stable stereotypes and the perception of reality in their context; the critical elements of crisis situations in social, technical, socio and technical systems of different origins prove the result of such effects.

In modern hybrid activities, information impact is dominant. It is realized in cyber space and through cyber space. They are directed to technical and erratic components of control systems with the help of information impact and impact on information. It combines informational, psychological and cyber components with the effect of its mutual intensification. The anticipating, early detection and the proper assessment of such impact and activities provide the opportunity of effective and adequate response. It stipulates the necessity of experience generalization and development of methods, means and tools of countermeasures against future and current hybrid effects and threats for providing a high level of our country's defence and defensive capacity of NATO members and partner countries.

Results of the research (Presentation of the main research material)

The increase of effectiveness of measures to ensure information and cyber security in cyberspace with the development of measures to counter hybrid influences can be achieved by solving a set of tasks:

1) Improvement of scientific applied and technological principles of design and realization of software and hardware means of cyber monitoring, protection, impact and its practical testing.
2) Designing the fundamental and scientifically applied base for development of hardware and software for providing monitoring, analytical information processing, forecasting, planning and conducting active and passive countermeasures against information threats in cyber space.
3) Designing and practical testing in the cyber range environment of software measures of monitoring, analytical information processing, forecasting, planning and conducting active and passive countermeasures against information threats in cyber space.
4) Innovative forms, methods and countermeasures against terroristic threats, of critical infrastructures protection, subjects and objects of command and control authorities in security and defence sector of the country, society and a person through the complex measures of information security in cyber space in conditions of hybrid conflicts of different intensity realization.
5) Designing of the methodological base for classification, standardization and certification of cyber ranges and the creation of classification system and cyber ranges standards.

The creation of the cyber range with the aim to investigate the complex cyber actions in the cyber space and through the cyberspace will provide the base for creation the powerful regional cyber centers and involvement of these structures in twenty-four-hour operational duty in the system of national and joint European information and cyber security using means and tools of the cyber range and the refinement of theoretical and applied principles of software and hardware development for countermeasures against hybrid impacts in cyber space.

The cyber range can be one of the effective means and tools for solving such problems.

The problem of design and implementation of laboratory environments for completing the exercises in cyber space is developed mainly in the creation of such cyber ranges: university (the type of cyber range KYPO, Masaryk University in Brno, Czech Republic); private civilian (according to the decisions of the company Forward Defense in Abu Dhabi city, organization of African Unity); national military (National Cyber Range in Orlando city, Florida, USA); international (NATO cyber range, Tallinn, Estonia) [17]. Hardware and software of mentioned cyber ranges are not aimed at providing functionally and technically the complex research of information influence of the technical and erratic components of control systems of different level and application. Within we may lose the research possibility of the synergetic effect of mutual reinforcement of psychological information and cyber impacts, which is realized and developed in cyber space. Traditional approaches are limited by research functions of mainly cyber threats. It doesn‘t involve the real experience of modern hybrid impacts. And it reduces the validity of received results.

The design and creation of the cyber range for the research and multilateral refinement of countermeasures against hybrid impacts in cyber space are realized with the help of common scientific methods of system analysis theory.

Practice proves that modern methods and ways of hybrid impacts realization are followed by significant traffic of dynamically changed critical situations. It is relevant for them the a priori uncertainty according to the target, subject and object of the impact, content, the essence and the way of the realization [18]. The technological design of the system of countermeasures against such critical situations, forms and ways of its application are aimed at static excessive system structure formation. The distribution of tasks to all components of the system executed evenly with a selection of elements according to its application. The increase of the quantity and density of the critical situations traffic and its types are worked out by the increase of structure elements. It produces informational redundancy of data, it's transmission and processing. The software of operational detection, protection and active countermeasures against information threats in cyber space are built on the same issues. These approaches are not effective in conditions of the real situation during the application of dominant or equal in content and development level of the enemy‘s information impact by information attacks.

The information mentioned above proves the relevance of the development of scientific approaches to the creation of the cyber range; its realization is directed to increase the effectiveness (complex criteria) of information security support in cyber space with the completion of the set of tasks of countermeasures against hybrid impacts according to partial criteria.

The aim of the article is to determine the methodical and applied aspects of designing, building and application of cyber range.

The cyber range is used as the technical component for complex research of the newest processes of information impact on technical and erratic components of control systems of different levels and application. Mutual intensification of mentioned impact types, which are realized and developed in cyberspace during cyber warfare, and real experience of combat actions are taken into consideration. It should be possible to use the integrated cyber range jointly with other existing analogues for improving their functional abilities [19]. In general, an integrated cyber range should provide: conducting the scientific research; training of personnel and development of education sphere; improvement of scientific research and educational bases; conducting the joint training; generalization of hybrid warfare experience and development of new forms, methods and tools of countermeasures to hybrid cyber threats.

Cyber range is a set of hardware and software measures, united by one distributed local net Internet access. It is intended for the refining the issues of designing, developing and testing the hardware and software systems (complexes) training for providing information security (psychological and information and cyber). The main purpose to use the cyber range is to increase the effectiveness of measures for providing information and cyber security in cyber space and the refinement of countermeasures against hybrid impacts. It is fulfilled during realization of monitoring functions, protection, passive and active countermeasures, conducting ambiguous training, providing experience generalization, developing forms, methods and measures of forecasting, prevention, detection and countermeasures of crisis situations in cyber space, conducting measures for practical training, retraining and postgraduate course for military (civilian) specialists (according to national and NATO Standards), research support for conducting fundamental and applied scientific researches in the sphere of information and cyber security of the country.

Specific complex cyber range should be created according to the ideology of open, distributed, complex, erratic, information control systems, invariant in their structure to the level of executed tasks. Technologies of protected computer nets are to be implemented in its structure and architecture. They have stationary and mobile sets of equipment with interchangeable, standardized modules. The control cycles are to be used as a functional base. They are Observation (information gathering from external and internal origins); Orientation (formation of the ambiguity of possible plans of actions and evaluation each of them according to a vector of criteria; Decision (the choice of the best plan for practical realization); Action (practical realization of the chosen plan of actions). It will provide the implementation of the model of independent situation control with its refinement in a time scale to near real-time traffic of crisis situations.

It is to design and produce an active cyber range from basic discrete components (Fig.1, 2) 1, 2.

The basic separate component of the cyber range includes two identical basic sets of specific hardware and software complexes according to their application, content, functional capabilities:

- a Set of Cyber Defense Forces;
- a Set of Testing Cyber Security Level.

A set of cyber defence forces are intended at providing cyber security of services, the data centre of a cyber range, security of its operators from information impacts through cyber space.

A set of testing cyber security level is intended at testing services of cyber range data centre and also for the evaluation of the operators‘ resistance to technologies of information impact through cyber space.

The cyber range includes a testing object. It is a powerful data centre, services, protected on the one hand by forces and measures of defensive capacity. From another hand, they are tested on cyber security by forces and measures of another set.

Separate components, mutual for both sets, are included in the cyber range. They are the subsystems of:

- a cluster of planning, organization and control of the cyber range work;
- a cluster of external cooperation;
- the subsystem of cyber security testing of data centre services.

Sets of cyber security defensive capacity and testing include subsystems:

- Cyber space and its components‘ analysis;
- Analysis and support of up-to-date databases of cyber incidents and cyber threats;

- Analysis of domain activities in cyber space;
- Analysis of activities in the blogosphere, social nets and mass media;
- Identifying and analysis of cyber technologies impact on control systems, network (physical and logical) topology, software and hardware of data centre services;
- Identifying and analysis of information impact technologies on datacenter operators through cyberspace;
- Identifying and analysis of technologies of information and cyber impact on critical elements of infrastructure components, security control sector and defensive capacity of the state, society and a person in conditions of hybrid conflicts of different intensity;
- Modelling of cyber security activities and means for wired and wireless networks of the data centre;
- Modelling of cyber security countermeasures against influences on control system, network (physical and logical) typology, hardware and software;
- Modelling of information protection of data centre operators through cyberspace;
- Identification and analysis of information and cyber technologies impact on critical elements of infrastructure components of security control sector and defensive capacity of the state, society and a person in conditions of hybrid conflicts of different intensity;
- Modelling of cyber security activities and means for wired and wireless networks of datacenter;
- Modelling of cyber security activities and means for control systems, network (physical and logical) topology, software and hardware of datacenter services;
- Modelling of information protection of datacenter operators through cyberspace;
- Modelling of cryptographic protection technologies;
- Modelling of information and cyber technologies impact on critical elements of infrastructure components of security control sector and defensive capacity of the state, society and a person in conditions of hybrid conflicts of different intensity;
- Modelling and simulation of actions in cyberspace, conducting training in cyber security and cyber defence;
- Modelling of cyber attacks on cryptosystems of datacenter;
- Modelling of socio-technical cyber attacks on datacenter operators through cyberspace, on security control sector and defensive capacity of the state, society and a person in conditions of hybrid conflicts of different intensity;
- Cyber security testing of datacenter services.

The scheme of cyber network typology is in Fig. 2 2. It includes sets, objects, components, clusters and subsystems of the cyber range, defined by the scheme in Fig. 1 1.

Fully functional scheme of the cyber range includes two basic discrete components. The design of each component can be fulfilled separately, in isolation, with the help of mutual approaches or with the designing results of exchange. The unification of two discrete components of structures (Fig. 1 1) according to the architecture (Fig. 2 2) is fulfilled by information unification in one cyber space. It was created by functionally unified internal (local), combined (locally global) and external (global) cyber spaces (Fig. 3 3). From a technological point of view, such unification is done on protocol levels of the corresponding type.

Suggested structure of fully functional complex cyber range gradually gains additional possibilities on three locally global levels of cyber space. It provides execution of forms, methods, measures, algorithms and technologies of cyber attacks identification, passive and active countermeasures, consequences elimination of cyber weapon use and renewal of normal network functioning of forces and weapon (armory), realization of monitoring and identification of threats, their analysis, forecasting, planning of executing active and passive countermeasures against information and psychological impact in cyber space and analysis of conducted measures effectiveness.

Hardware and software resources of *the testing subsystem on cyber protection* (cyber security) should provide the possibility of conducting cyber impacts of different types. It is to involve corresponding network protocols, vulnerabilities of systematic and applied software support, antivirus software defects. For example, port scanning, refuse in maintenance, monitoring and information interception in network channels, pseudo authorized insinuation in *the subsystem of security*, destruction, distortion, information pilfering (theft), access denial to it in the cyber defense subsystem with the help of special measures of software impact etc.. Technical devices and specific software are to provide reliable protection of system resources and information. They are circulating and are being stored in the computers of the local network of the cyber defence subsystem.

In the framework of the cyber range information security specialist (each one separately or in defined teams) will have the possibility to execute special techniques of cyber attacks and protection from them. And it will not harm the existing electronic infrastructure of the state.

The structure of fully functional cyber range provides autonomous, multi-sided and multi-levelled simultaneous target orders execution according to real conditions.

To design and create the cyber range the following tasks should be realized:

- improvement of applied scientific and technological principles of design and realization of hardware and software cyber means of monitoring, security and impact for the creation of the cyber range;
- design of the structure and detailed architecture of the cyber range according to designed applied scientific and technological principles of its construction;
- creation of two discrete components of the cyber range from its two basic sets according to the scheme and architecture (Fig.1, 2) 1, 2, providing the functioning support (adjustment, testing)

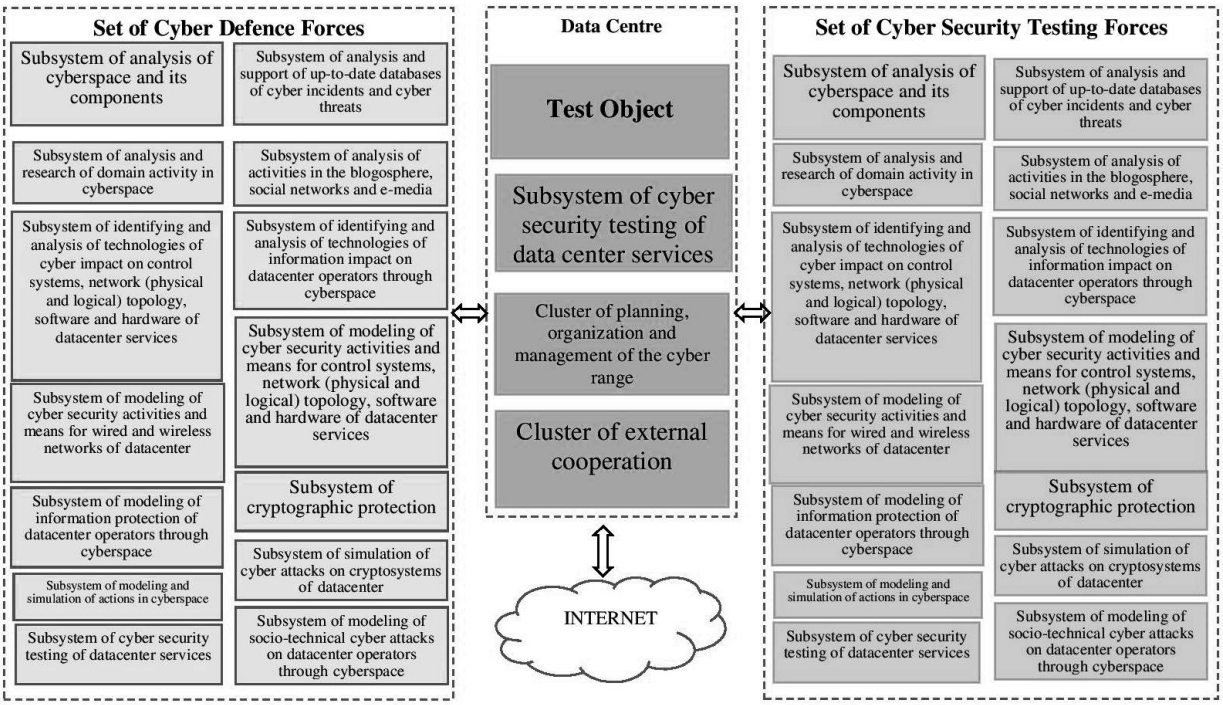

Fig. 1. Structure of the Cyber Range Scheme

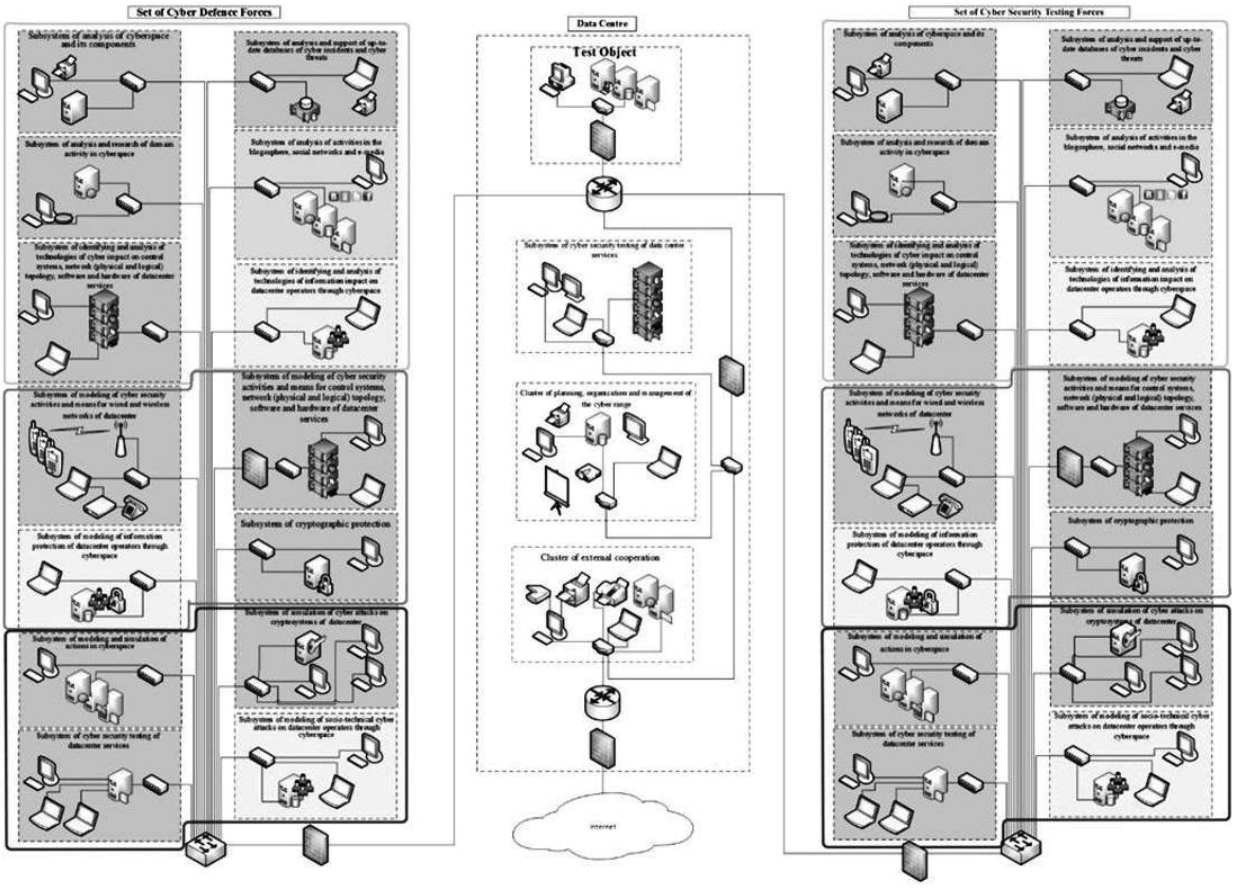

Fig. 2. Cyber Range Network Typology

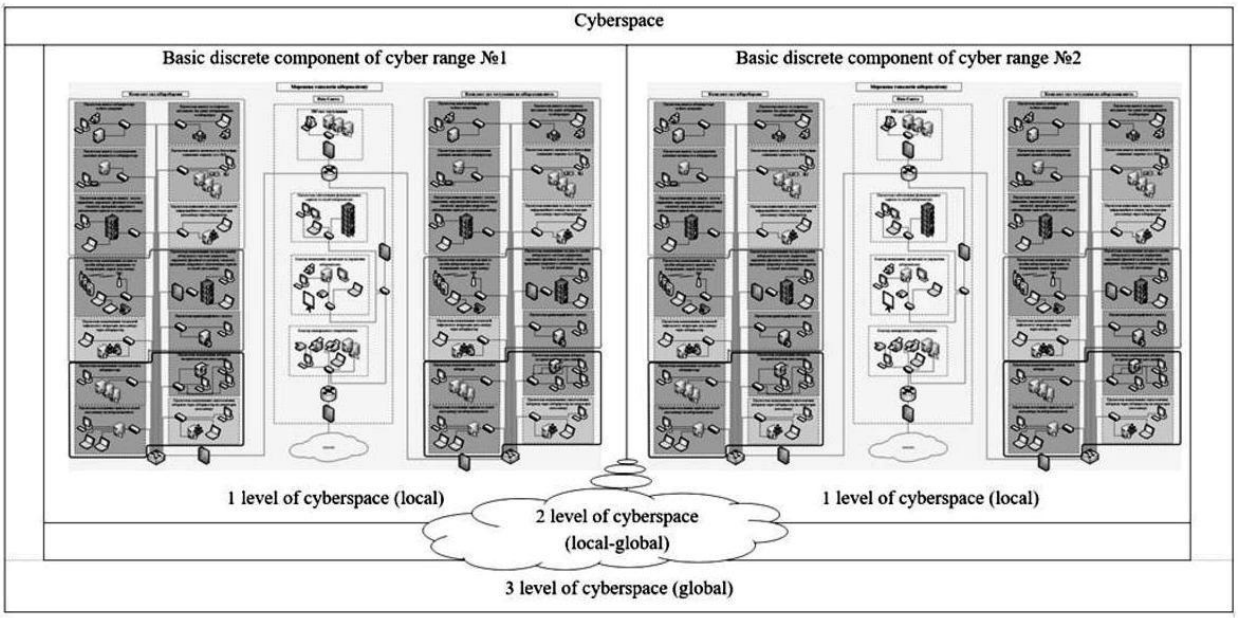

Fig. 3. Structural Scheme of Fully Functional Cyber Range

of the first local level of cyber space according to the categories of decompositional division (Fig. 3) 3;
- creation of fully functional complex cyber range by information unification of created discrete components into one information space; it functions and creates internal, combined (local-global) and external cyber space components;
- design of the program and methodology of the cyber range testing according to fully functional structure and architecture.

The countermeasures against hybrid impacts are executed in cyber space for the effective fulfilment of sets of measures of information and cyber security. It also stipulates the design of methodological support of monitoring processes realization, analytical information processing, forecasting, planning and executing passive and active countermeasures against cyber threats in cyber space. Conditions of prior uncertainty, traffic density of destructive impacts and significant dynamics of crisis situations involve situation control methods, fractal analysis, self-organizing and bifurcated models. It is stipulated to implement principles of situation control of hardware and software space of the cyber range. The sets of processes and methods providing information and cyber security are conducted in the cyber range. These processes are dynamic and cyclic. They are realized according to concrete crisis situation on the chosen list of necessary and decent elements from available components of the cyber range. The complex of functional information connected virtual subsystems is created for this purpose. These subsystems are called information control clusters (ICC). They execute tasks consequentially and in parallel. Such ICC are situationally synthetized for identification, localization and liquidation of concrete crisis situations. Mentioned issues are realized in a form of situational structurally parametric synthesis of the complex distributed information control system. In this way, the process of situation control of the structure and cyber range parameters is realized. This procedure provides timely spacious, structural and functional distribution of task execution of traffic density of destructive impacts in significant dynamics of crisis situations. Also, the regularity of partial tasks of information processing and download in the data transmitting channels is reduced. As a practical result we will receive the effective reaction on traffic density of dynamically changed destructive impacts in conditions of significant dynamics of crisis situations with qualities of prior uncertainty by the subject and object of the impact, content, essence and method of realization; task orders execution in time scale close to real and to high criteria of probability and completeness of output information.

Implementation of situation control principles for effective task execution in the cyber range needs fundamental and applied researches. The results of these researches are going to be the concept of situation control of the structure and parameters of hardware and software space of the cyber range for effective task execution. It provides information security in cyber space in conditions of significant traffic density of dynamically changed destructive impacts in significant dynamics of crisis situations with the quality of prior uncertainty.

On each ICC a set of processes is conducted and is realized on the base of:

1) The method of cluster search and information arrangement about information threats in cyber space;
2) Methods of crisis situation identification in conditions of its traffic density and dynamics of changes with principles of self-organizing implementation;
3) Methods of automated operational and fundamental integrated information analysis of monitoring;

4) Methods of forecasting the ICC development and threats in the information sphere using bifurcated models;
5) Methodological approaches of fractal construction of hardware and software assets of automated passive and active information (psychologically information psychological, cyber) protection.

To achieve the above-mentioned results we need to solve the number of issues. It is supposed to be achieved in three stages.

The first stage is designing of fundamental and applied bases for constructing mathematical support of software and hardware assets for the realization of monitoring processes, analytical information processing, forecasting, planning and implementation of passive and active countermeasures against information and cyber threats in cyber space.

During the execution of this task, it is stipulated to apply all the scientific results mentioned above. They are of the scientific base for the design of software assets of monitoring processes realization, analytical information processing, planning and conducting active and passive countermeasures against information threats in cyber space.

The second stage is: designing and practical testing of software realization assets of monitoring processes, analytical information processing, forecasting, planning and conducting of passive and active countermeasures against information and cyber threats in cyber space.

The essence of this stage is in the design of hardware and software assets, a set of software additions, computer programs, models etc. They are based on designed fundamental and applied bases for constructing mathematical support of software and hardware assets for the realization of monitoring processes, analytical information processing, forecasting, planning and conducting of passive and active countermeasures against information and cyber threats in cyber space for effective resistance against hybrid impacts.

To achieve the above-mentioned results it is necessary to solve the following tasks:

- Situation control of the structure and parameters of cyber range hardware and software space;
- Cluster search and information arrangement about information threats in cyber space;
- Crisis situation identification in conditions of its traffic density and dynamics of changes with principles of self-organizing implementation;
- Automated operational and fundamental integrated information analysis of monitoring;
- Forecasting the ICC development and threats in the information sphere using bifurcated models;
- Planning of countermeasures against information threats in cyber space and evaluation of their effectiveness;
- Cyber impact and protection from unauthorized access to information and telecommunication systems;
- Organizing laboratory space for conducting special researches in the sphere of technical and cyber security assets;
- Defining the best method of threats neutralization in cyber space concerning existing hardware and software assets of technical information protection;
- Modelling information telecommunication systems attack and protection processes of critical infrastructure objects;
- Security level evaluation of electronic resources, hardware and software assets of information telecommunication systems;
- Analysis of cyber impact effectiveness of information telecommunication systems of critical infrastructure objects of an adverse party.

The design of software support with mentioned functions is stipulated with the use of construction technologies of intellectual expert systems, support systems of decision making, geoinformation systems under up-to-date conditions, technologies and spaces of high-level software coding.

Designed hardware and software assets are an indispensable component of the cyber range.

In order to get it done we need:

- a set of hardware and software assets, a set of software additions, models etc., which realize the functions that are mentioned above with software documents on them;
- testing programs and methods of designed hardware and software assets, a set of software additions, models etc. for use on different levels of cyber space (according to the categories Fig. 3 3);
- testing results of designed hardware and software sets, a set of software additions, models etc., on the first and the second levels of cyber space (according to the categories Fig. 3 3).

The third stage is the development of innovative forms, methods and countermeasures against challenges and threats of terrorism, critical infrastructure protection, protection of society, state and defence sector control, of a person through the realization of information protection methods in cyber space directed to countermeasures against hybrid impacts;

The essence of this stage is in the realization of practical tasks based on the seminatural modelling with the implementation of principles and techniques of game theory, the antagonistic conflict between conditionally opposing forces. They act on their basic discrete components of the cyber range. The scenarios are designed according to the objectives of the researches. Recording results of the cyber range activities, their posterior analysis provide production of innovative forms, methods and countermeasures against challenges and threats of terrorism, critical infrastructures protection, protection of society, authorities, and a person. Mentioned information is illustrated in the scheme Fig. 4 4.

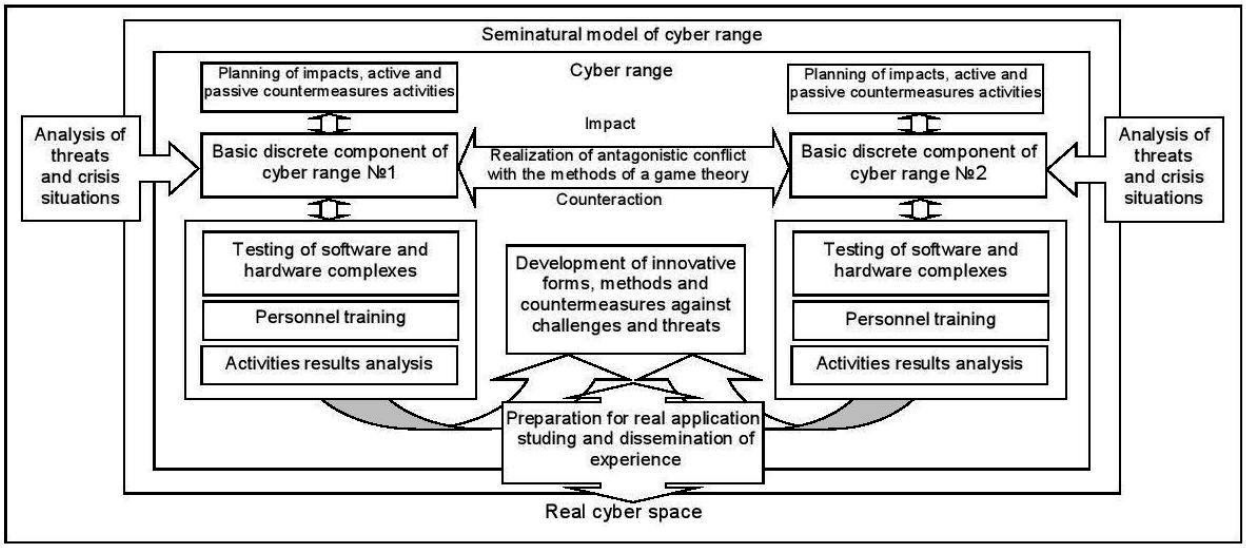

Fig. 4. Scheme of innovative forms, methods and countermeasures against information threats in cyber space development

The results are going to be the following:

1) Methods and scenarios of conducting ambiguous training in the cyber range in supporting information security in cyber space;
2) The active set of cyber range hardware and software assets for complex execution of information security tasks (information, psychological and cyber security) with possibilities of its standardization and certification;
3) Methods of personal training support systems of information and cyber security, gained by personal skills and knowledge;
4) Testing results of designed hardware and software sets, a set of software additions, models etc. on the third level of cyber space (according to the categories Fig. 3 3) in conditions close to real use;
5) Innovative forms, methods, countermeasures against challenges and threats of terrorism, critical infrastructures protection, protection of society, state authorities and its defence sector, personal protection with the help of a set of measures realization of information security in cyber space directed to countermeasures against hybrid impacts;
6) Executed theoretical and applied tasks, hardware and software component, highly qualified specialists will become the base for creating a powerful cyber centre. It will conduct twenty-four-hour operational duty in the system of national and Common European information and cyber security.

Development of science and research base in the sphere of information security, conducting ambiguous national and international training, improvement of the training system, retraining and postgraduate courses of military specialists in the sphere of information security with the implementation of NATO Standards and increasing the time of practical training.

The execution of mentioned tasks is in conducting organizational measures by the use and implementation of the results and experience of the previous task execution. In particular:

- conducting ambiguous national and international training in the sphere of information and cyber security with improvement and design of innovative countermeasures against new and forecasted threats, implementation of NATO Standards and increasing the time of practical training, achieving compatibility of Armed Forces of Ukraine with NATO member countries in the sphere of information and cyber security;
- implementation of new directions of perspective fundamental and applied scientific researches with use of emergent properties of the active cyber range. It combines methods of seminatural modelling, principles and techniques of game theory, antagonistic conflict, directed to integrated researches of information (psychological, information) security problems in cyber space for countermeasures against hybrid impacts;
- making recommendations in improving the content and methods of the training system, retraining and postgraduate courses of military and civilian specialists in the sphere of information and cyber security in NATO partner and member countries according to national standards and NATO Standards etc.

The execution of the mentioned tasks will provide an increase of the information and cyber security effectiveness in cyber space by executing the countermeasures against hybrid impacts. It is achieved by the design and production of the active set of the complex cyber range. It involves the training of ambiguous practical measures with the design of innovative forms and countermeasures against challenges and threats of terrorism,

critical infrastructures protection, protection of society, state authorities and a person.

The complex cyber range totally differs from existing analogues. One of the main differences is in the unification of information impact researches on technical and erratic components of control systems of different levels and application (state, critical objects, armed forces, weapon etc.). It concerns also the synergetic effect of mutual reinforcement of mentioned impact categories. They are realized and developed in cyber space during conducting hybrid actions.

The main peculiarity of hardware and software component of the cyber range is in the implementation of situation control principles, fractal analysis, self-organizing, bifurcated models. They provide effective task completion of information (psychological, information) and cyber space security in conditions of prior uncertainty, traffic density of destructive impacts and significant dynamics of crisis situations in the information sphere. It is relevant to modern hybrid conflicts.

The suggested approach is appropriate to the complex cyber range application as scientific and research space for testing, researching forms and countermeasures against hybrid impacts, personnel training, development of applied scientific directions of hardware and software base improvement. It doesn‘t intervene in the existing information structure of the state. It concerns the synergy of psychological and information and cyber impacts. It is supported by real practical experience. But the peculiarity of the cyber range functional application is that the intervention into the real system is excluded.

Active results in task realization of analysis and synthesis of complex systems, information automated storing, processing and analysis in conditions of prior uncertainty, traffic density and significant dynamics of critical situations provide the application of synergetic methods. In particular, they are methods of situation control, fractal analysis, self-organizing, bifurcated models etc. Implementation of situation control principles gives an opportunity to rational distribution and redistribution of own resources and forces concentration on critical directions of the enemy‘s actions. Fractal analysis, self-organizing, bifurcated models methods help to identify threats and critical situations, prevent the direction of their development. In practice, it provides an increase of countermeasures effectiveness against information impacts by advancing the enemy in time, completeness and authenticity of information, during the reacting and during the actions.

Conclusions

Aspects of cybernetic destructive actions in modern wars and armed conflicts are investigated on the basis of the analysis of the features of the hybrid war. It is substantiated that the provision of effective counteraction to destructive cybernetic influences requires the availability of cyber range. Definitions, principles and concept of construction of a complex cyber range for the study of hybrid cyber actions are proposed, as well as a list of problems to be solved to create a complex cyber range. The questions of methodology and applied aspects of the creation and application of complex cyber range are considered. The basic structure and procedure for the practical creation and use of a comprehensive cyber range are presented.

Prospects for research. Formation of the requirements for the structure and content of databases and knowledge bases of the proposed cyber range based on the results of its practical application and research of functioning during the specified tasks activities.

References

[1] Y. Danyk, T. Maliarchuk, and C. Briggs, “Hybrid war: High-tech, information and cyber conflicts, connections,” *The Quarterly Journal*, vol. 16, no. 2, pp. 5–24, 2017. URL: http://www.jstor.org/stable/26326478.

[2] Y. Danyk, Y. Katkov, and M. Pichugin, *National security: avoiding of critical situations. Monograph: National University of Defense of Ukraine.* Zhytomyr, Ukraine: Korolyov Zhytomyr Military Institute, 2006.

[3] F. Hoffman, “Hybrid warfare and challenges,” *Joint Forces Quarterly*, no. 52, 2009.

[4] B. Boyer, “Countering hybrid threats in cyberspace,” *Cyber Defense Review*, vol. 2, 2015. Ed. 3.

[5] A. Clarke, “Cyber war: The next threat to national security and what to do about it by richard,” 2010. [Online]. Available: `http://indianstrategicknowledgeonline.com/web/Cyber_War_The_Next_Threat_to_National_Security_and_What_to_Do_About_It_(Richard_A_Clarke)_(2010).pdf`.

[6] S. Harris, *Cyberwar : The Fifth Theater of War.* 2014.

[7] B. Renz and H. Smith, “Russia and hybrid warfare – going beyond the label,” 2016. [Online]. Available: `http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf`.

[8] P. Eronen, “Russian hybrid warfare: How to confront a new challenge to the west,” *FDD PRESS*, 6 2016.

[9] I. P. III, C. Paul, and M. York, “Redefining information warfare boundaries for an army in a wireless world,” 2016. [Online]. Available: `https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf`.

[10] J. Suler, “The online disinhibition effect,” *CyberPsychology and Behavior*, no. 7, 2004.

[11] M. Mateski, C. Trevino, and C. Veitch, “Cyber threat metrics,” *Sandia National Laboratories Report*, 3 2012.

[12] “What is cyber threat intelligence, and why you need it,” 1 2017. [Online]. Available: `https://blog.unloq.io/what-is-cyber-threat-intelligence-and-why-you-need-it-fd33e24954da`.

[13] P. Cornish, R. Hughes, and D. Livingstone, "Cybers space and the national security of the united kingdom. threats and responses," *A Chatham House Report*, 3 2009.

[14] "Cyberspace threats and vulnerabilities," 1 2017. [Online]. Available: http://www.informationclearinghouse.info/pdf/cyber_warfare_case_for_action.pdf.

[15] Y. Danyk, "State cyber defense formation and development in conditions of hybrid challenges and threats," *International Conference on Information and Telecommunication Technologies and Radio Electronics. September. 11-15, 2017*, 9 2017. DOI: https://doi.org/10.1109/UkrMiCo.2017.8095427.

[16] Y. Danyk and S. Gudz, "Special operations for disruption of state and military control system," *Security and Defence Quarterly, published by War Studies University, Warsaw, Poland*, no. 4, 2015. URL: https://securityanddefence.pl/resources/html/article/details?id=124640.

[17] Y. Danyk and R. Grischuk, *Fundamentals of Cyber Security: Monograph; in general edited by prof. Yu.G. Danyk*. Zhytomyr: ZHNAEU, 2016. 636 P.

[18] O. Pysarchuk, "Conception of identification of the controlled situations on basis of self-organization of heterogeneous signs," *Cybernetics and computing technology*, no. 178, pp. 66–81, 2014.

[19] Y. Danyk and A. Pisarchuk, "Method of structural parametric synthesis of complex erratic distributed informational - controlling system of response on conflict situation," *Journal of automation and information sciences, Begell Hours, inc. publishers*, vol. 46, no. 3, pp. 47–69, 2014. USA INS 1064-2315.