SUMMARY
OF THE SCIENTIFIC WORKS
Of Ph.D. Angel Genchev

The research works are in the areas of automated control systems, information processing methods, artificial intelligence, modern information systems and technologies, modelling and decision support, teamwork systems, cybersecurity, digital communications and others. The developments include implemented information task solutions, subsystems and systems for the needs of defence in the field of operational and combat support, communication and information support, decision support systems, systems for automation of military management, modelling systems, etc. The research projects are related to the design of information and communication systems for the needs of the leadership of the Ministry of Defence and the Bulgarian Army and their subordinate structures, as well as departmental projects to support the country's governance in crises, natural disasters and others.

The scientific works are presented in three categories:

I. Monographic works

II. Scientific articles and reports

III. Research and development activity

I. MONOGRAPHIC WORKS

1.1 R. Iliev, A. Genchev **MODERN DATA CENTERS (REQUIREMENTS, TECH-NOLOGY, BUILDING**). Monograph, Edition of “Professor Tsvetan Lazarov” Defence Institute, ISBN 978-619-90024-3-8, Sofia, 2021, 273 pps. (Reviewers: Professor DSc Veselin Tselkov, University of Library Studies and Information Technologies and Col. Assoc. Prof. Dr. Eng. Mario Angelov, "Professor Tsvetan Lazarov" Defence Institute.

The monograph examines modern data centres - the invisible to users of information and communication services a set of infrastructure, technologies, systems, software and computer devices. The book provides an overview of the historical development and stages that data centres go through, since the emergence of electronic computers, and attention is paid to the first data centres in Bulgaria (known under this name until the 90s). of the twentieth century). The development *and the main types of modern data centres, their general architectural features, as well as the sequence of their construction are analysed. The evaluation and conclusions of the research of the most used technological platforms for building data centres offered by Vmware and Microsoft, as well as many Linux-based solutions, such as Red Hat Virtualization, Xen Cloud platform, Proxmox virtual environment and others. Basic criteria for selection of a software platform for virtualization are proposed, such as cost of ownership, required number of virtual machines, supported operating systems, systems for ensuring high access to services and resources, assessment of the degree of workload and others.*

The monograph presents the basic standards and good practices for building data centres, the requirements and recommendations of the American Telecommunication Industry Association (TIA) and its standard ANSI/TIA-942, aimed at the telecommunications infrastructure of data centres.

Some innovative solutions of companies in the field for the creation of different types of data centres - modular, mobile, environmental, and attention is paid to the rapid growth and construction of new data centres not only on land but also underwater. (Microsoft Experimental Data Centre), especially after the expansion of the epidemiological situation in 2020 - 2021, when remote communication, learning and working from home was widely practiced.

An essential part of the monograph is devoted to the creation of a conceptual model for building a system of data centres for the needs of security and defence, including a large number of operational, functional, technical, technological, informational, organizational and others. requirements for it.

The described model, requirements and technology of work on the implementation of the system of data centres are the result of research and experiments of the authors with popular software platforms for virtualization, as well as the experience with various hardware devices for system configuration, obtained thanks to their working prototype of a cloud data centre at the Institute of Defence.

II. SCIENTIFIC ARTICLES AND REPORTS

II.2.1 N. Stoyanov, A. Genchev, R. Iliev **SOME ASPECTS IN THE RISK ANALYSIS IN INFORMATION SECURITY AND DEFENSE SYSTEMS.** Scientific Conference of the University of Shumen "Bishop Konstantin Preslavski", Proceedings, 2009, pp. 200-209

The report presents some aspects of risk analysis in information systems. Definitions, sources and other parameters that affect the risk of C4I systems are considered. The results of this study were used in building communication systems for the Bulgarian Army.

II.2.2. R. Iliev, N. Stoyanov, A. Genchev. **An architectural approach in creating of an information environment for collaboration**, Scientific Conference of the University of Shumen "Bishop Konstantin Preslavski", Proceedings, pp. 214-221, 2009

The report proposes an approach to creating an information environment for collaboration, based on the application of three types of architectural views - functional (operational), systemic and technical. An implementation of such environment for joint work of officials in one organization (successfully tested in structures by the Ministry of Defence) through the application of modern information technologies and technical solutions has been proposed.

II.2.3. A. Genchev, R. Iliev, N. Stoyanov**. Study of the possibility for application of diskless workstations in the information systems of the Bulgarian Army**, Scientific Conference of the University of Shumen "Bishop Konstantin Preslavski", Proceedings, pp. 210-213, 2009

The report presents the results of a study based on the use of an information network of diskless workstations for the exchange of classified information, which integrates modern methods, tools and systems for information protection. The researched technological solutions for creating such a network are presented and conclusions are made about those that allow to significantly improve the security of information processed in the information systems of the Bulgarian Army in compliance with the requirements set out in the law and its provisions.

II.2.4. Genchev A., **Advanced technologies and solutions for intelligent defense**. Scientific Conference with International Participation "MT & S-2011" Proceedings, ISBN 978-619-90024-1-4, Sofia, 2012, pp. 101 - 105.

The report analyses the NATO Secretary's Smart Defence initiative presented in his speech at the Munich Security and Defence Conference (February 4, 2011). The concepts are derived from it and are adapted to the modern IT technologies. Proposed are examples of solutions implementing these concepts.

II.2.5. Genchev A., **Analysis of virtualization systems towards the construction of cloud architectures**. Scientific Conference with International Participation "MT & S-2013", ISSN 2367-5942, Sofia, 2014, Proceedings, II-25 - II-40

The report reflects the results of a study conducted in the course of work on a systematic project "Development and modernization of the Integrated Information Infrastructure of BA". The possibilities and limitations of the modern virtualization and cloud infrastructure management systems from leading manufacturers and those with open source code are considered in order to use the results in selecting an appropriate platform for the needs of the project.

II.2.6. Genchev A., **Optimization of the usage of hardware resources**. CIO Magazine issue from 2015 - July.

The report presents in a very concise form the results of a 2-month research, experimentation and development of systems that allow the sharing of one computer system by several users. The developed system relies on virtualization to create a complete illusion of each user for his own hardware, while protecting his information from the other users and protecting the virtualization solution from access with administrative rights. It saves computer hardware and RAM by implementing the KSM (kernel same page merging) subsystem, which has been in the Linux kernel for some time. The implementation was successfully experimented in two configurations in the Directorate "Administrative and Information Provision" in MOD-1, and a distribution medium (DVD) was provided for the system administrator.

II.2.7. Kolev A, Genchev A. **The Institute of Defense implemented a hybrid model of IS in a virtual environment**. CIO Magazine, issue from 2018 - July.

The report examines issues related to inherent limitations in the storage of large volumes of data. An improved, "hybrid" model of organization of the data storage subsystem, proposed by the authors, is implemented. The report demonstrates the idea of combining the use of virtualization of part of the resources of the computer system - where it has the desired effect (such as isolation of individual *applications) with the use of non-virtualized resources such as disk memory. The idea has been realized also in practice - as an information system - an electronic library for the needs of BDI.*

II.2.8. Iliev R., Genchev A. **BUILDING A SYSTEM OF DATA CENTERS FOR THE NEEDS OF DEFENSE.** International Scientific Conference "Hemus 2018", Proceedings, II-189 - II-195, Plovdiv, 2018

The report examines some modern solutions for building data centres and analyses various criteria for selecting platforms for virtualization and creating cloud environments focused on their use for defence purposes. The possibilities for building a system of data centres for the needs of defence are presented, as well as some specific requirements that they must meet.

II.2.9. Genchev A., Iliev R. **ACQUISITION OF SENSORY INFORMATION FROM UNMANNED AIRCRAFT FOR ASSESMENT OF A CRISIS ENVIRONMENT**. International Scientific Conference "Hemus 2018", Proceedings, II-153 - II-162, Plovdiv, 2018.

The report examines the problems encountered in collecting sensory information from unmanned aerial vehicles in crisis situations and suggests ways to overcome them.

II.2.10. Genchev, A., R. Iliev. **INFORMATION PROTECTION AND CYBER SECURITY OF CORPORATE INFORMATION SYSTEMS**. International Scientific Conference "Hemus 2018", Proceedings, II-163 - II-173, Plovdiv, 2018

The report provides an overview of possible modern cyber attacks, methods and means of protection against them, applicable to corporate information systems. Schemes for protection of corporate systems from different types of impacts through the application of existing software products are proposed.

II.2.11. Genchev A. **Sensors and sensor technology used in unmanned aerial vehicles**. . International Scientific Conference "Hemus 2018", Proceedings,, II-174 - II-188, Plovdiv, 2018.

The report reflects a part/consecutive step of the work on research and development of a system for acquisition and visualization of sensory information under programs 7.1, 7.2 and 1.7.7 of the Ministry of Defence. It contains a study of the types of sensors used in unmanned aerial vehicles, sets requirements for them and their communication interfaces in order to build a system for collecting and transmitting data in real time from the scene of a crisis event.

II.2.12. P. Nikolova, Genchev, A. **Analysis and visualization in case of possible cyber-attacks**. 2018, International Scientific Conference "Hemus 2018", Proceedings, II-107 - II-114, Plovdiv, 2018.

The report contains an analysis of tools for detecting and preventing cyber-attacks. Based on this analysis, a relational model is proposed for a database management system for storing information about cyber-attacks against a specially prepared sensor - honeypot. The methods for geo-referencing the sources of cyberattacks are considered and on this basis a solution is proposed for their visualization on an electronic geographic map.

II.2.13. Iliev, R., A. Genchev. **POSSIBILITIES FOR USING UNMANNED AERIAL VEHICLES TO OBTAIN SENSORY INFORMATION FOR ENVIRONMENTAL ANALYSIS**. Information & Security: An International Journal 46, no. 2 (2020): 127-140, https://doi.org/10.11610/isij.4609

This article presents some possibilities for obtaining sensory data from the environment (such as meteorological data, pollution level, radiation, etc.), using unmanned aerial vehicles (UAVs). Attention is paid to specific requirements for UAVs used as flying platforms for sensory data collection. The process of creating a prototype of a system for collecting and transmitting data in real time from the scene of a crisis event using UAVs is analysed. It is proposed to use a specialized neural network set up to identify half-hidden (half-covered by disaster) people when analysing images obtained from UAV sensors flying over the scene of a crisis event.

II.2.14. Genchev, A., R. Iliev. **USING UNMANNED AERIAL VEHICLES FOR COLLECTION AND TRANSMISSION OF DATA IN REAL TIME FROM THE PLACE OF CRISIS EVENT**. SPRINGER 2021 Communications in Computer and Information Science (series), ISSN: 1865-0929, 2020

The report analysis the possibilities of using unmanned aerial vehicles (UAVs) to obtain sensory data from the scene of a crisis event by assessing their flight, communication and sensory capabilities. An approach is proposed for the use of UAVs for prevention and assistance of rescue teams in assessing the crisis situation by equipping such a device with an appropriate system of sensors, communications, means for primary data processing and more. The report proposes to use a specialized neural network to be used to identify semi-hidden people after analysing their images. Some of the results obtained are illustrated.

II.2.15. Genchev A. **Development of budget-oriented solutions for IP telephony, intended for the military formations of the Bulgarian Army.** Hemus 2020 International Scientific Conference, Proceedings, II-165 - II-172, Plovdiv, 2020

The report presents the results of the development of a prototype of a field digital IP-PBX based on open source software solutions. A block diagram of the interaction of the software components and an example scheme of connecting instances of the PBX to forma a larger IP-telephony network are given. A study of the possibility of connecting the IP PBX to the existing ISDN infrastructure by building a bridge to ISDN-E1 lines both through an additional component and by installing an E1 interface module in the hardware of the PBX is presented.

II.2.16. Iliev, R., A. Genchev. **GENERALIZED NET MODEL OF THE DECISION MAKING PROCESS IN THE CRISIS MANAGEMENT.** Journal 'Advanced Studies in Contemporary Mathematics', South Korea, 335/839(39.9%) in the category of mathematics (The 2011 SJR in SCOPUS for Advanced Studies in Contemporary Mathematics is 0.043 with a ranking) (for print)

The article presents an unpublished until now model of the decision-making process in crisis management with the help of a generalized network, implemented with five transitions. To assess the feasibility of the decision, the last transition takes into account the fact that not all generated crisis management solutions can be successfully implemented. When evaluating the parameters of the individual nuclei, the possibility of using fuzzy and intuitionist fuzzy values is provided for more accurate modelling of the process and clearer presentation of the purely human way of expression.

II.2.17. A. Genchev. **A CONCEPTUAL MODEL FOR WEB PAGE MONITORING SOLUTION**. 2021, International Conference on Advanced Research and Technology for Defence (ARTDef).
In the fight against cybercrime and in particular the defacement of WEB pages, it is necessary to monitor and timely inform the responsible staff. The report presents an analysis of the problem and approaches to solving it using open source tools. The proposed approach involves the use of a WEB browser core to ensure the correct reproduction of the content of WEB pages that rely on AJAX and Javascript to be displayed.

II.2.18. A. Genchev. **Visualization of sensory information received from unmanned aerial vehicles at a crisis management center**. 2021, International Conference on Advanced Research and Technology for Defence (ARTDef).

The report reflects another stage in a series of developments that began with research and selection of a suitable flight platform and analysis of the necessary sensors and solutions for determining the location in 3-D space. The visualization *solutions used in the control center are presented, which includes the construction of a video wall and a WEB software application for visualization of a 3-D model of the terrain and the data from the sensors.*

II.2.19. Genchev A. **Adaptive algorithm for dynamic allocation of frequency resources, applicable in cellular communication networks with special purpose**. International Conference on Advanced Research and Technology for Defence (ARTDef) proceedings 2021.

In the course of research on adaptive algorithms for dynamic frequency allocation for reuse in cellular radio networks, it was found that there is a need to create an adaptive to intentional interference and at the same time, decentralized algorithm. In addition, it is necessary for the algorithm to continue to function in case of loss of part of the neighbouring cells or communication with them. This report presents a proposal for such an algorithm.

II.2.20. Vasilis Katos, Angel Genchev, Maya Bozhilova and Nikolai Stoianov, **Cybersecurity user requirements analysis: the ECHO approach.** 2021, "Lecture Notes in Networks and Systems" (ISSN: 2367-3389) Vol. 344 (MODS-2021 June 28-July 1, 2021)

The report presents a structured approach to identifying knowledge about cybersecurity and extracting users' needs based on the development of specific use cases. Sample descriptions of use cases of attacks on a common computer network are given. The proposed use cases are analysed in the CAIRIS platform. The modelling process confirms that CAIRIS is a powerful tool for enriching the context of threat models and UML class diagrams. Also, CAIRIS modelling can support the use of design security principles. The study is part of the European Network of Cyber Security Centres and Innovation and Operations Competence Centre (ECHO) project.

II.2.21. A. Genchev, M. Bozhilova, N. Stoianov. **Multi-sector cyber security analysis methodology – the ECHO approach**. 2021, DIGILIENCE 2021

The report presents a structured methodology for identifying sector knowledge of cybersecurity, analysing consumer needs and deriving sector-specific uses, designed to address task 2.5 of the ECHO project. An example is given in the field of defence for the application of the proposed methodology, as well as a verification approach. The study was conducted within the project "European Network of Cyber Security Centres and Innovation and Operations Competence Centre" (ECHO).

III. RESEARCH AND DEVELOPMENT ACTIVITY

A. Applied developments

3.1. Command and control information system

The automated command and control information system has national scope and is designed to support crisis management of various kinds. It includes several subsystems and provides over 60 information and communication services based on four main computer networks. Developed by R. Iliev (supervisor), N. Stoyanov, A. Genchev, H. Radev, D. Zhelyazkov, N. Lazarova, A. Tsolova. Implemented research and applied development, adopted in BA in 2008.

B. National projects, system descriptions, manuals

3.2. Information system "Information equipment of operational premises".

The document is a technical project for equipping the work premises of the operational staff with modern information-technical and software tools for work. A technical specification is also included. The project is developed on the basis of conducted research and experiments in the field of ACS and application of modern IT-technologies and solutions, by a team consisting of: R. Iliev (head), N. Stoyanov, A. Genchev, H. Radev, AGK , 2009

3.3. Information Network "AIM-AGK"

Technical project for construction of an automated information network of AGK for the work of officials, providing a wide range of information and communication services (joint work with electronic documents, electronic calendar and time schedule, tools for planning activities, IP-video telephony, e-mail, etc.). Technical specification is also included in the project. The project was developed on the basis of conducted research and experiments on the application of modern IT technologies and solutions by: R. Iliev, N. Stoyanov and A. Genchev, AGK, 2008.

3.4. AIS of BA. Information and communication environment for joint work and support of the management process

The document is a project for the development of the Automated Information System of the Bulgarian Academy of Sciences. The project was developed in order to develop the AIS of the BA and provide officials from the MoD and the BA with modern information and communication services to support the management process and in connection with the integration of systems developed by external MoD developers. It is an application of modern information and communication technologies, researched, analysed and experimented by the team, developer of the project. Describes the construction of information and communication environment are joint work of officials, which includes the following more important subsystems: subsystem for group work; communications and video conferencing; geographic information subsystem; supporting emergency management; decision support; messaging and notification subsystem. The project was developed in 2011 by R. Iliev in its main part (as noted in the introduction), and some points are the work of: I. Hristozov, N. Stoyanov, A. Genchev, A. Borisov, G. Georgiev , K. Andreev, A. Atanasov, D. Karakolev. The project was approved by the Armaments Council for implementation.

3.5. Development and modernization of the Integrated Information Infrastructure of the Ministry of Defense (MOD)

The document is a systematic project for development and modernization of the Integrated Information Infrastructure of the Ministry of Defense through the implementation of modern information and communication technologies and solutions for building server architectures. The project is an application of a number of studies and analyzes of modern achievements of IT technologies and their application in practice. The project was developed in 2011 by N. Stoyanov (head), R. Iliev, I. Ivanov, S. Stoykov, A. Genchev, M. Bozhilova, A. Kolev. The project was approved by the Armaments Council for implementation.

3.6. Development and modernization of the Integrated Information Infrastructure of the Bulgarian Army (BA)

The document is a systematic project for development and modernization of the Integrated Information Infrastructure of the BA through the implementation of modern information and communication technologies and solutions for building server architectures. The project is an application of a number of studies and *analyzes of modern achievements of IT technologies and their application in practice. The project was developed in 2011 by N. Stoyanov (head), R. Iliev, I. Ivanov, S. Stoykov, A. Genchev, M. Bozhilova, A. Kolev. The project was approved by the Armaments Council for implementation.*

3.7. Center for Research and Development of ICIS and C4I Systems. Cyber Attacks and Information Security Laboratory

The project aims to provide scientific support, construction, testing and development of information and communication systems and C4I systems for the needs of defence and security of the country. It is designed to provide a research and laboratory base for the analysis, research, training and implementation of cyber-attacks, as well as to increase the security of communication and information systems and networks for the needs of ICIS and C4I systems, in accordance with the priority investment projects of the Long-Term Investment Plan-Program of the Ministry of Defence. The project is implemented on the basis of research and analysis of promising IT technologies worldwide, which should be experimented with and on their basis to make future developments for the needs of the Ministry of Defence and the Armed Forces. The project was developed in 2011 by N. Stoyanov (head), I. Ivanov, R. Iliev, A. Genchev, M. Bozhilova.

3.8. Center for Research and Development of ICIS and C4I Systems. Laboratory "Training and training ground for CIS, information protection and command and control systems"

The project aims to provide scientific support, construction, testing and development of information and communication systems and C4I systems for the needs of defence and security of the country. It is designed to provide a research base for training and conducting training on CIS, information protection systems and C2-systems of ICIS and C4I-systems in the priority investment projects of The long-term investment plan-program of the Ministry of Defence. The project is implemented on the basis of research and analysis of promising IT technologies worldwide, which should be experimented with and based on them to make future developments for the needs of the Ministry of Defence and the Armed Forces. The project was developed in 2011 by I. Ivanov (head), N. Stoyanov, R. Iliev, A. Genchev, A. Kolev.

3.9. Opportunities for using open source office suites in the Bulgarian Army

The aim of the study is to study and test various software office products (with free licenses) to be used in the Bulgarian Army. The document includes: identification of software packages with a freeware license, which will be alternatives to commercial office packages; analysis of compatibility with Microsoft Office in terms of user interface and file formats; analysis of the general functionality of the applications; stability testing; study of the ways in which the prospects for development of each of the products are maintained; analysis of the experience of EU countries and proposals for future research.

The study was conducted by a working team consisting of: A. Genchev, R. Iliev, M. Bozhilova.

C. EDUCATIONAL AND METHODICAL WORKS
(TID, TTZ, programs, methodologies, etc.)

This section includes educational and methodological works related to the author's participation in the development of technical and economic reports, tactical and technical assignments, programs and methods for testing and acceptance of automated information tasks, complexes, subsystems and systems, as well as of other source documents necessary for the acquisition of computer products for the needs of the Ministry of Defense, the Bulgarian Army and their subordinate structures.

In 2013, a technical and economic report on the development of the corporate information system for defense (387 pages) was developed, including a comprehensive study of existing systems, technologies, solutions and global trends in building such systems and upgrading them to cloud. infrastructure.

The document was developed by: G. Velev (head), R. Iliev, A. Genchev, N. Stoyanov, M. Angelov, I. Ivanov, I. Hristozov, J. Yordanov, G. Grancharov.

In 2014, a tactical and technical task (121 pages) was prepared for the construction of the system (by G. Velev, A. Genchev and R. Iliev), based on the application of modern cloud technologies and information environments for joint work. adopted by the Armaments Council).