SUMMARIES

of scientific papers related to the competition of Ch. Assistant Professor Dr. Eng. Rosen Stefanov Radkov for a participation in a competition for Associate Professor academic position in the professional field5.3. Communication and Computer Equipment (discipline: Computer Networks and Internet) at the Department of Software and Internet Technologies in the Faculty of Computer Sciences and Automation,announce in State Gazette No. 65/06.08.2021.

For participation in the competition are presented 23 (twenty three) scientific papers, representing a habilitation thesis - a monograph, publications in scientific journals and published reports presented at scientific forums and a guide for laboratory exercises in the discipline "Internet servers and services".

The scientific publications are divided into three groups, in accordance with indicators В.3, Г.7 and Г.8 of the document "5. Detailed reference for compliance with the minimum national requirements'.

Indicator Г.7 includes **4** (four) scientific publications in publications that are referenced and indexed in the Scopus scientific information database, of which **2** (two) are independent. The publications are divided into the following groups:

- Publications in collections of reports in Bulgaria, referred to in Scopus - **4**;

Indicator Г.8 includes **17** (seventeen) scientific publications in unreferenced journals with scientific review or in edited collective volumes of which **14** (forty) are independent.

According to the type of publication, the publications are divided into the following groups:
- Publications in magazines published in Bulgaria - **8**;
- Publications in collections of reports in Bulgaria - **6**;
- Publications in collections of reports abroad - **3**;

According to the topic, the total number of publications is divided into the following groups:
- Design and evaluation of the reliability and quality of data centers - **11**
- Computer Science - **4**
Information security, personal data protection and information security management systems
- E - learning - **1**

By language of publication:
- In Bulgarian - **14**
- In English - **8**

[Indicator B.3] Habilitation thesis - monograph

[B.3] Radkov, Rosen. Continuity of information security. Analysis and management approaches. Varna, TU-Varna. 2021. 130 p. ISBN:978-954-20-0828-6

The monograph clarifies the essence of the concepts of information and data, as well as their importance for both organizations and individuals. The principles that must be followed to ensure the security of the information are clarified. An exposition of the aspects related to ensuring the continuity of business processes and the security of the information processed in them is made. The need to introduce a management system is justified. The normative documents are described, which regulate the requirements to the information security management systems, through the implementation of which the security of the information and its continuity is guaranteed. The essence of the management systems is clarified and the information related to their certification in accordance with the international standards is summarized.

Based on audits conducted in various organizations, an analysis of the management of the continuity of information security in carrying out activities in them. As a result of the performed analysis the following conclusions are drawn:

1. The implementation of ISMS in accordance with the requirements of ISO / IEC 27001 is recommended when an organization wants to improve the management of information security, but it is not enough if it does not understand deep enough its requirements, as well as the essence and the peculiarities of the applied technologies;

2. The ISO / IEC 27001 standard is well accepted in all economic sectors

3. There is no difference in the process of managing the continuity of information security, regardless of the type (private, collocated or rented) of the corporate data center;

4. Serious weaknesses have been identified in the process of business impact analysis, in particular on information security, which has a significant impact on the planning and management of information security and, as a consequence, on ensuring its continuity;

5. Weaknesses have been identified in the planning and implementation of the disaster recovery process. The processes of planning and maintaining the process of information security continuity are analyzed.

An approach has been created that supports the process of creating a BCDR plan and aims to take into account all the circumstances and features that contribute to the creation of a quality BCDR plan. The presented approach is universal and can be used both for the purposes of supporting the process of managing the continuity of information security and in managing the continuity of activities. The proposed approach is adapted for practical application.

[Indicator Г.7] Scientific publications in publications that are referenced and indexed in world-famous databases of scientific information.

AN APPROACH TO CHOOSING AN OPTIMAL IT INFRASTRUCTURE IN ACCORDANCE WITH AN ASSIGNOR'S REQUIREMENTS

Rosen Radkov

The report presents an approach developed by the author to select the optimal IT infrastructure based on the requirements of the client. The need to create an approach is due to the fact that despite the existence of international and established national standards for the structure, design and operation of data centers (DCs) and their IT infrastructures (ITIS), which are successfully applied in the design and implementation of large data centers, then in organizations of the type of micro, small or medium enterprises there are difficulties in determining the ITIS of the DC they need. There is no unified approach on the basis of which they can evaluate the solutions offered to them and take a reasoned and adequate to their needs decision on the composition of the ITIS of their DC, to be implemented.

The presented approach solves the task of assessing the quality of DC and the selection of the appropriate ITIS in accordance with the requirements of the contracting authority. For this purpose, a set of pre-developed reference ITIS is used. Their quality is assessed by calculating six indicators, which are justified as the most important. It is necessary for the contracting authority to determine the desired values of the six indicators, as well as their coefficients of significance. The next step in the approach is to determine the "ideal ITIS" that has the best indicators. For all ITIS, the reference, the ideal and the contracting authority, a complex quality indicator is determined using the formula for a complex geometric indicator. As a result of the work of the approach is the choice of one of the reference ITIS as the most suitable for the contracting authority. This is the reference ITIS, whose value of the complex indicator is the closest, but greater, than the value calculated for the desired ITIS by the contracting authority. In case of a negative difference, it is necessary to make a change in the input parameters and repeat the calculations.

The approach is adapted for practical application. Software tools have been developed for its application. There is no limit to the number of predefined reference ITIS. It was used in the design of seven data centers.

The nature of the indicators used is such that any businessman or manager of an organization can easily identify them without the need for technical knowledge.

The approach can be applied not only when designing a highly reliable data center, but also when assessing the quality of an existing data center.

ARE DISASTER RECOVERY LEVELS SUFFICIENT TO ASSESS THE DATA CENTER'S DISASTER PREPAREDNESS?

Rosen Stefanov Radkov and Ivan Dimitrov Dimitrov

The modern world is highly dependent on information technology to manage business processes in companies, in state and local government, healthcare, education and even to provide comfort at home. It is crucial for any organization to ensure the business continuity and rapid disaster recovery. There are classifications for assessing the level of IT infrastructures according to their disaster recovery capabilities.

In this report, the authors critically analyze these classifications and demonstrate that they are outdated and insufficient to determine whether the risks associated with the operation of IT infrastructures are covered. It is proposed to include additional indicators in the assessment of the resilience of IT infrastructures against disasters, which take into account not only the technical solutions applied in IT infrastructures, but also organizational aspects, such as the organization of its operation, segregation of duties and the need for more frequent updating. of the assessment approach to take into account new technologies, changes in the environment and new threats to the functioning of IT infrastructure.

REFERENCE HIGHLY RELIABLE IT INFRASTRUCTURES FOR THE MICRO-, SMALL- AND MEDIUM-SIZED COMPANIES

Rosen Stefanov Radkov

Designing a data center (DC) is a complex task. When it is necessary to design a data center for the needs of companies of micro, small and medium business, there is a difficulty in choosing the appropriate data center.

This report presents three reference IT infrastructures (ITIS) with high reliability, which are used in an approach developed by the author (published in another report), through which a reasonable choice is made of the optimal IT infrastructure on behalf of the contracting authority. The calculated values of their unit quality indicators are presented.

The developed reference IT infrastructures (RITIS) are highly reliable, which is evidenced by the values of the calculated single quality indicators for each of them. The goals to be achieved with the respective ITIS are defined. Each of them is a set not only of hardware and software, but also of organizational measures that regulate the management of DC and information security. Without these organizational measures, the values of some of the single quality indicators will be worse.

The developed reference ITIS can be used not only in the approach developed by the author for selection of optimal ITIS according to the assignment of the assignor, but also as a guide for building a highly reliable DC. Depending on the specifics of the respective project, on the basis of the same RITIS, implementations can be obtained by applying different hardware and software components.

E-LEARNING IN THE COVID-19 CONTEXT - EPIDEMIOLOGICAL AND EDUCATIONAL CHALLENGES

Radkov Rosen Stefanov, Radkova Zhaneta Grigorova, Vankova Desislava Ivanova, Petkova Yulka Petkova

Technologies have transformed education gradually and forever. Oppositely, Coronavirus (COVID-19) has changed education suddenly and temporarily (assuming). However, the pandemic context has facilitated the wider introduction of technologies in the conservative academic environments in Bulgaria.

The report analyzes both social and educational issues in the context of COVID-19. Challenges in e-learning are considered from an objective and subjective point of view, as well as from a technological point of view. Good examples from the practice of dealing with situations depending on the specifics of the studied disciplines are presented. Some suggestions for building an appropriate infrastructure for e-learning are presented. In addition, examples are given in the academic fields of computer science and public health.

The report identifies and answers the following research questions: What is different in e-learning in the 2020-pandemic context? What problems and challenges did we face? How to improve e-learning and alleviate the damages of the social isolation? The overall aim of this article is to classify and analyze e-learning challenges in the context of COVID-19 and to propose solutions.

The idea of the current discussion is to promote and support the sustainable integration of the digital technologies in the Bulgarian colleges and universities. The authors are university teachers and have to cope with emerging educational challenges on a daily basis. Therefore, the proposed strategies are practice-oriented. The development of technological literacy has become not only a personal responsibility but a social imperative.

COVID-19 demanded changes in the short-term and academia has responded. However, long-term reshaping in curricula, teaching approaches and research agenda are pending. COVID-19 pandemic could be viewed as an opportunity for "great realization". Indisputably, the future belongs to the brave but not egocentric, to the e-literate but also professionally competent. The upcoming 2020/2021 academic year will happen in an extraordinary times and we have to be ready!

[Indicator Г.8] Scientific publications in unreferenced journals with scientific review in Bulgaria and edited collective volumes in Bulgaria

Scientific publications in edited collective volumes in Bulgaria

[Г.8.1] **Radkov R.**., Kolev S., Network router. Scientific-thematic collection of UNS. T. 2. 1995, 471-479. Anniversary scientific session with international participation, 22-23 May **1995**, AFA "G. Benkovski" Dolna Mitropolia.

NETWORK ROUTER

R. S. Radkov, S. G. Kolev

The publication highlights the growing need to data transfer between different types of devices. Data transmission networks have been set up. Thus a new direction of science was formed, which developed extremely fast. The creation and management of computer networks requires the use of a new technical base, new principles of transmission and switching. The problems that arise when connecting computer networks with different architectures are defined. Overcoming these differences is done by building interconnection nodes that connect the networks of a certain layer of their architecture.

The publication describes the architecture of a designed hardware-software device of the network router type. The operation of the software is analyzed using a specially written program that analyzes the execution times of the CPU32 + processor instructions, taking into account its pipeline organization and taking into account the execution time of the instructions from the RISC processor.

The designed device allows without changes in its hardware configuration, to add new capabilities for managing communication devices. The management procedures set out in the PPP and SLIP protocols have been successfully tested.

[Г.8.2] **Radkov R.**., Antonov P.., Ethernet switch design problems, Proceedings. T. 3. 1999, 138-144. Eighth National Scientific and Applied Conference „Electronic technique ET-99", Sozopol, 23-25 September **1999**.

ETHERNET SWITCH DESIGN PROBLEMS

Rosen Radkov, Petar Antonov

The publication discusses the increasing trends in the market of Ethernet platforms for local area networks, as well as the requirements for the efficiency of their operation. It has been concluded that for a number of practical applications, a single-segment Ethernet configuration or an extended repeater configuration is insufficient, and in most cases it is necessary to break the network into several segments using bridges or switches.

The report discusses methodological problems of designing Ethernet switches for specific purposes. Given the complexity of these devices, at the design stage it is proposed to develop a block diagram of the hardware and related software, then with the help of analytical and / or simulation model to analyze the probabilistic-temporal characteristics of operation and to specify the necessary buffer memory capacity and CPU speed. A mathematical model has been proposed to describe the operation of the switch. There are two separate phases in the model: (1) a single-channel system with an expectation for servicing the total Poisson flow, and (2) a multi-channel queuing system. Dependences on the probability of frames loss and the average residence time of the frames are derived.

HIGHLY RELIABLE DATA CENTER FOR HEALTH INFORMATION

Rosen Radkov

The care for human health requires the use of new applied technologies, with the help of which the values of certain indicators are constantly monitored, which are recorded by devices specially developed for this purpose. The report proposes a reasoned solution for a highly reliable data center needed for reliable data collection, processing and storage in a Patient Monitoring Center (PMC).

It is defined that the design and construction of an IT solution that satisfies the above functionalities requires the application of modern hardware and software technologies. Determining the composition of DC, optimal for each case, requires setting the values of certain indicators. After analysis of the required quality of the data center (DC) for PMC and risk assessment, their values are determined. A model of the data center is created and the composition of its components is described. The goals set in the design of the DC are described. The author's approach, subject of another publication, for the design of DC is applied and the DC, which is necessary in order to meet the set requirements, is determined.

The quality indicators of the designed data center have been calculated and it has been proven that they meet the set requirements. It is concluded that:

• Providing better treatment and addressing the challenges associated with health problems caused by high levels of stress and other factors requires the use of applied technologies ensuring constant monitoring of patients in hospital organizations.

• Their successful implementation requires reliable data collection, processing and storage, as well as their constant availability.

• The presented solution provides 99.9048% availability or eight hours and twenty minutes of unavailability for one year.

• The implementation of planned and unplanned maintenance takes place without the need to turn off the equipment.

• The possibility for easy expansion of DC when increasing the volume of data or the need to take on tasks related to new processes.

[Г.8.4] **Radkov R**., Technological solutions for achieving compliance with GDPR. Proceedings. 2018, 218-229. Sixth National Seminar on "European Citizens and Intellectual Property, Perception, Awareness, Behavior", ULSIT, 25-26 April **2018**, ISBN 978-619-185-350-2

TECHNOLOGICAL SOLUTIONS TO ACHIEVE COMPLIANCE WITH GDPR
Rosen Radkov

The publication analyzes the requirements introduced by the new regulation adopted by the European Union for the protection of individuals with regard to the processing of their personal data. The new challenges for the organizations affected by it are identified, which are related to the need to make detailed analyzes of the implementation processes in which organizations collect and process personal data, as a result of which to develop and implement adequate organizational and technical measures. The question is raised: What are the technological solutions, through the application of which, the organizations will carry out the processing of personal data in accordance with the requirements of the regulation?

The report analyzes the requirements of the regulation that can be met by introducing technical measures and examines the applicable technological solutions. The wide variety of technological solutions is discussed and the report analyzes the possibilities to achieve compliance with the regulation by applying blockchain technologies, known for the anonymity of the subjects.

The specific technological solutions that can be applied in IT infrastructures (ITIS) in order to achieve compliance with certain requirements of the regulation are considered. It is defined that the choice of a specific technological solution is not trivial and the same for all organizations. It depends on the size and structure of the organization, as well as the amount of data that is collected and processed. The solution is different for each organization because it depends on the nature of its business processes. It is determined that the right decision is the result of the implementation of a sequence of several steps: it begins with an analysis of business processes, determining the personal data of individuals used in them, why they need to be processed, who processes them and when and where they are stored; a risk assessment is performed in relation to personal data and a review of the controls applied to date in the organization to minimize the risk; on the basis of the obtained results a choice of technological solutions is made, with the help of which to improve the current ITIS and to achieve the satisfaction of the requirements of the regulation.

The described technological solutions and the defined steps for their implementation can be used as a guide supporting the process of implementation of the measures for meeting the requirements of the regulation.

ORGANIZATIONAL AND TECHNICAL MEASURES TO ENSURE COMPLIANCE WITH GDPR

Rosen S. Radkov

The report examines the basic principles of personal data protection introduced by Regulation 2016/679 adopted on 27 April 2016 by the European Union. The regulation set a number of new requirements for data controllers and operators (PDCOs). One of the main goals of its introduction is to harmonize the legislation in the EU member states regarding the protection of individuals with regard to the processing of their personal data and ensuring the free movement of such data. The deadline for its implementation, May 25, 2018, provides a period of two years during which organizations to take the necessary measures to bring the way they process personal data of individuals in accordance with its requirements. PDCO needs to make adequate changes to existing procedures or create new ones, as well as to find the right solutions in cases where the requirements of the regulation conflict with other regulations or legal provisions. To ensure compliance with the regulation, PDCO needs to implement appropriate technical means for personal data protection. The scope of the measures to be implemented depends on the information security controls already in place. This report proposes a process approach, the application of which will help the process of compliance with the new regulation. The technical measures that need to be applied in order to meet the requirements of specific clauses in the regulation are also defined. As a result of the analysis of the Regulation on personal data protection, it was concluded that in order to ensure compliance with Regulation 2016/679 of the European Union, PDCO needs to:

- apply the process-oriented approach as proposed in this report;
- introduce and implement organizational measures;
- apply adequate technical hardware and software;
- realize that the application of technical measures alone is not enough;
- provide support from management;
- carry out a constant assessment of the work of the introduced controls and make a decision for their improvement.

[Г.8.6] **Radkov R.** Analysis of personal data protection and intellectual property in information security management systems. ULSIT, 26 April **2021** (in print)

ANALYSIS OF PERSONAL DATA PROTECTION AND INTELLECTUAL PROPERTY IN INFORMATION SECURITY MANAGEMENT SYSTEMS
Rosen Radkov

The protection of personal data is an issue whose relevance is timeless, but with the ubiquitous development of the Internet, the introduction of IT technologies in any business process and the growing volume of information exchanged within an organization and between organizations, requires more and more great attention. It is necessary to take into account the changes in the legal framework both nationally and in Europe and worldwide. The report analyzes the personal data processed in many organizations, as well as the measures that have been implemented to ensure their protection. The applied ways for identification and satisfaction of the applicable legal and contractual requirements regarding intellectual property rights are also analyzed. The normative acts and documents that are up-to-date for the current period of time have been determined. The analysis is based on the results of an audit of information security management systems conducted in organizations of different business sectors, size and ownership. The typical weaknesses that are allowed are identified and recommendations for their elimination are given. Seven areas for improvement have been identified that organizations need to consider in order to bring their information security management systems into a state that will ensure real protection of personal data and intellectual property.

Научни публикации в редактирани колективни томове в чужбина

[Г.8.7]   **Radkov R**., Selecting the optimal IT infrastructure of a data center, Proceedings of the 1st International Conference Applied Computer Technologies ACT 2018, Ohrid, Macedonia, 21-23 June **2018**, pp.26-29, ISBN 978-608-66225-0-3

SELECTING THE OPTIMAL IT INFRASTRUCTURE OF A DATA CENTER
Rosen Radkov

The successful operation of any organization in the modern world depends on the quality of the data center services used for this purpose. In order to meet the quality requirements of the services provided, it is necessary to make an appropriate design of the architecture and the correct selection of the components used. Choosing the optimal IT infrastructure (ITIS) for the data center (DC) needed for the work of any organization is a complex issue. Its complexity is a result of the contradiction that exists between the price of the required investment and the price that the organization wants to pay. The higher the quality and the more reliable the IT infrastructure, the higher its price. On the other hand, it makes no sense to invest in a lower cost IT infrastructure that does not meet the requirements of the organization and its business processes.

This report demonstrates the use of an author's approach to selecting the optimal IT infrastructure and analyzes its operation.

The application of the approach for selection of the optimal ITIS for solving a specific task is presented. It is demonstrated that the difficulty of solving a problem of this nature can be overcome and reduced to setting values for six indicators, the nature of which is such that any businessman or manager of an organization can easily define them without the need for specific technical knowledge.

The way of analyzing the results and evaluating the possibilities for changing the input parameters if necessary is demonstrated.

[Г.8.8] **Radkov R**., Analysis and evaluation of a Data Center quality indicators. Proceedings of 15-th International Conference on Informatics and Information technologies CIIT2018, Mavrovo, Macedonia, 20-22 April **2018** pp.173-178, ISBN 978-608-4699-08-8, http://ciit.finki.ukim.mk/

ANALYSIS AND EVALUATION OF DATA CENTER QUALITY INDICATORS
Rosen Radkov

It is difficult to imagine the modern world without the presence of information technology. They are all around us. We use them when we are at work, when we are resting and even when we are having fun. Each IT infrastructure (ITIS) changes during its operation due to a change in the values of various indicators: number of hours worked of its components, volume of processed and stored data, number of users served, changes in business process requirements, destabilizing environmental factors and others. The following questions arise for the organizations for which ITIS has been built:

• How to make sure that the built ITIS has the qualities set in the project?

• How to ensure continuous maintenance of high quality of services provided by ITIS?

This report presents an author's approach to finding answers to the questions asked. The components of a typical IT infrastructure are presented. Selected and substantiated are some of the most important indicators for assessing the quality of a data center - accessibility and workload. The dependencies of these on other indicators of the data center are substantiated.

Monitoring and analysis of the work of a specific ITIS has been performed. For this purpose, appropriate monitoring systems have been installed and data have been collected for a period of half a year. It can be seen that the achieved availability of the system for the observed period is 99.977%, and the load of its individual components is below 16%. It follows that during the observed period of operation of the system it has worked according to preliminary expectations, has the ability to service new business processes and allows maintenance and planned maintenance without interrupting business processes.

In conclusion, it can be argued that the application of the proposed approach to analyze the functioning of ITIS makes it possible to obtain real results for the operation of the system. From their analysis it can be concluded whether the quality indicators of the implemented ITIS correspond to the values set in the project, as well as whether the set quality of the services is continuously ensured.

EXTERNAL FACTORS DESTABILIZING THE OPERATION OF DATA CENTERS

Rosen Radkov

Ensuring the integrity and accessibility of information is one of the most important tasks in the field of information technology. This is due to the dependence that business processes have on the IT infrastructure (ITIS), which ensures their implementation. The current conditions of the business environment are such that this dependence is almost 100%, and require ITIS to provide an acceptable interruption of business processes, which in most cases, especially when talking about an organization belonging to the big business, is reduced to a few minutes and even seconds.

The report analyzes the external destabilizing factors that affect the work of a data center. Based on the analysis of the individual components of data center (DC) and the peculiarities of their functioning and the external factors influencing their work, an environmental model has been created, including the main threats to the integrity and availability of data, destabilizing factors that may cause assigned to the relevant disaster category. The use of the presented model would help to prepare a risk assessment in which to identify all sources of risk by identifying possible threats, the likelihood of their occurrence and potential consequences. The purpose of this step is to generate a comprehensive list of risks based on events that could affect the operation of the DC.

The analysis of the impact of the environment on the work of DC shows the need to assess the risk of occurrence of each of its destabilizing factors. Based on this assessment, adequate decisions can be made about the composition of the DC and the organization of its management so that the organization that uses the DC is protected from violating the integrity and accessibility of its data and all the negative consequences that would have if not such protection.

The application of the proposed model of the environment in the risk assessment makes it possible to include all potential threats to the work of DC.

Научни публикации в нереферирани списания с научно рецензиране в България

HIGH RELIABILITY DATA CENTER FOR CARDIOLOGY INFORMATION
R. Radkov, Y. Yotov

The publication discusses the importance of the issue of patient information, which doctors need to fight to solve the problem of heart failure as the final stage of all heart disease. The need for centralized processing of this information is justified. It requires the creation of a database with a high level of access and continuity of operation, the practical implementation of which is carried out through the establishment of a Center for Monitoring Patients with Heart Failure (CMPHF). The successful operation of the CMPHF depends on the provision of reliable processing, storage and backup of cardiac data. A technical solution for the construction of a highly reliable data center is presented, ensuring the operation of the monitoring center and the data that need to be reliably collected, processed and stored are defined.

The described architecture is an IT solution with centralized storage and processing of information, control of network traffic, implementation of a solution for replication of information, as well as a system for backup and archiving of information.

A reliable model has been created by applying the connectivity models and the quality indicators of the IT infrastructure have been calculated. The presented solution guarantees the necessary availability of DC 99.99% (fifty-two minutes per year) and acceptable data loss and is built through a highly reliable designed architecture and application of modern IT solutions. The performance of prophylaxis of the hardware and software part of the data center (DC) is carried out without interruption of the work processes in the CMPHF. Possibilities for easy expansion of DC are provided in case of increase of the volume of work and the processed data.

ASPECTS OF PERSONAL DATA PROTECTION IN HANDLING CARDIAC DATA

R. Radkov, Y. Yotov

Heart failure as the final stage of all heart disease is a problem that requires a doctor to have a large amount of information related to the condition of patients. The processes of consultation, diagnosis and treatment are related to the processing of special categories of personal data, which must be brought in line with the general regulation on data protection of individuals, adopted on 4 May 2016 and effective from 25 May 2018. The report clarifies the mandatory requirements that need to be met and makes recommendations for the applicable organizational and technical measures to comply with the Regulation.

The requirements of the law presuppose the developers of software products to submit solutions that bring the developed software products in line with the principles set out in the regulation 2016/679. Applicable measures include the use of anonymization, pseudonymization and data encryption, as well as the introduction of control over access to information through the application of a directory service, identity management, the introduction of an access matrix, the application of document management systems and more.

Dealing with the problem of heart failure requires individual continuous and long-term monitoring of a number of clinical, laboratory and instrumental parameters, which, regardless of where they are performed, are related to the treatment of patients' personal data.

The analysis of the requirements set by the regulation 2016/679 shows that achieving compliance with them is possible only as a result of the introduction of adequate organizational and technical measures. The greatest success will be if a system based on a process-oriented approach is introduced for the processing of personal data. Successful compliance with the regulation 2016/679 can be ensured only if there is support from the management and if it is realized that the application of technical measures alone is not enough, as well as that a continuous evaluation of the work of the introduced controls must be performed. the results of the management and decision-making for their improvement.

These measures must be creatively implemented so as not to hinder and interfere with the work of health professionals.

DATA MODEL CENTER FOR MICRO, SMALL AND MEDIUM BUSINESS COMPANIES
Rosen Radkov

The report reports that micro, small and medium-sized enterprises (SMEs) statistically represent more than 90% of the total number of companies and create every two out of three jobs. The data centers (DCs) of these companies represent the core of their IT infrastructure and are especially important for the functioning of work processes. A challenge for IT specialists is the construction of a data center that will ensure the smooth and resistant to external destabilizing factors of the business processes in the company.

Depending on the specifics of each of the three types of companies, the difference in their IT infrastructures is described, and as a result of summarizing the characteristics of the companies a generalized model of data center is proposed to be used in designing its IT infrastructure.

The proposed model describes not only the software and hardware components of DC, but also activities related to the implementation of policies for its management and information security management. The services necessary for his work are also indicated. Following the proposed DC model, highly reliable data center (HRDC) can be successfully designed for SMEs. The main differences in the IT infrastructures of the three types of companies classified as SMEs are due to differences in the number of business processes served, the number of users and the amount of data they work with, the number of sites and their geographical location. These differences have a significant impact on both the required computing power and the IT concepts and solutions applied in the data center.

METHODOLOGY FOR ENSURING HIGH RELIABILITY
THE DATA CENTER

Rosen S. Radkov

Data centers ensure the operation of business processes in organizations and companies. As a result of their work, citizens and companies get the opportunity to use the applications used by the business process and the services generated by it. An important condition for providing quality services is to ensure high reliability of the data center. This article analyzes the solutions for creating high reliability and offers a methodology for its provision.

Currently, there are many standards and good practices for the design and construction of DC or parts of its infrastructure, but there is a lack of methodology to describe the actions and activities that need to be performed to ensure a highly reliable data center (HRDC).

The report proposes a methodology to help organizations and companies solve this task in an optimal way. From its content it is clear that the implementation of a solution for HRDC is carried out not only through the design and implementation of highly reliable IT infrastructure and a set of plans and procedures, but also through staff training, training and evaluation of the system. The proposed methodology is adapted for practical application.

[Г.8.14] **Radkov R.** Analysis and comparison of international standards for data centers. Computer science and Technologies. Varna, Technical University of Varna. **2017**, 8-16. ISSN 1312-3335

ANALYSIS AND COMPARISON OF INTERNATIONAL STANDARDS FOR DATA CENTERS

Rosen S. Radkov

The report substantiates the importance of data centers (DCs) for business and the need to take into account not only the requirements of business processes, but also the requirements of international and national standards when designing and building them. This article analyzes the standards and determines their applicability in solving the individual tasks solved in the design and construction of DCs, as it is important that the specialists who design and build DCs are familiar with existing standards and good practices.

Currently, there are many standards for the design and construction of DC or parts of its infrastructure. The purpose of this article is to determine which of the data center standards should be followed when designing and building a DC or part of its infrastructure.

As a result of the analysis, it was concluded that only EN 50600-X and ANSI / BICSI 002 address all aspects of design, implementation and maintenance. Only EN 50600-X defines the minimum design requirements, but ANSI / BICSI 002 provides the most comprehensive information that can be used as recommendations and good practices. DCs must be standardized and certified. This helps those interested to find the right answer to many questions, for example: what type of DC business model to choose, how much money to invest in DC, how to choose the right DC supplier, etc.

INTERNATIONAL SCIENTIFIC COMMUNICATIONS ON THE PROBLEMS OF PATIENT'S ELECTRONIC MEDICAL RECORD AND CLOUD TECHNOLOGIES

Росен Радков

The report analyzes the use of cloud technologies for healthcare in the last ten years. It is reported that their application in the development of an electronic patient file and access to it is gaining more and more popularity in the practice of medical institutions.

A scientometric study of the dynamics of international scientific communications on this issue has been conducted and a significant increase in recent years of publications and discussions on this topic has been established. The publications referred to in the Web of Science Core Collection (WoS) and Scopus databases during the period between 1999 and 2018, incl. The leading countries, authors and magazines during this period are highlighted. The results show the constant interest of the world scientific community in this socially significant issue, aimed at further optimization of health care systems.

From the analysis and used literature the managers of the medical establishments can get information about the use of the cloud technologies in the field of the electronic health file, and the scientists and the heads determining the scientific policy in our country can increase the efficiency of their scientific activity and the international visibility of their achieved.

SOFTWARE DEFINED NETWORKS – A BRIEF STUDY

Rosen S. Radkov

Modern computer networks are complex to manage, and adapting to new business requirements and problems is very difficult. This article presents a brief study of the new computer network management technology called Software Defined Networks (SDN). In this paper are expailed motivation of their creation, their main concepts and trends of their development. Software Defined Networks separate from each other the functional layers of a computer network - data plane from control plane. This functionality enhances the programming capability, flexibility and manageability of the network. A study on the forecasts for the development of SDN networks is presented and the main requirements they must meet are defined.

Because traditional networks are complex, they are difficult to manage. The development of cloud services is difficult with the traditional way of managing networks. Software-defined networks create the ability to make network management easier and smarter. In addition to separating the data plane from the management plane in the network architecture, they also include centralized network management. This allows network management to be performed directly by applications using the API without the need to know the network architecture in detail. Along with the wonderful ideas built into SDN, there are new challenges related to the reliability, scalability and security of SDN.

SECURITY AND PRIVACY OF PATIENT'S ELECTRONIC MEDICAL RECORD DATA - A DYNAMIC INSTITUTIONALIZATION OF RESEARCH ON THESE PROBLEMS

Rosen Radkov

The report summarizes the issues related to the creation, maintenance and use of the electronic patient file. In recent years, data security and confidentiality have been a major focus in building and using the patient's electronic file. Globally, a number of standards have been introduced for best practices and recommendations for information security management, risk assessment and the introduction of controls in information security management systems.

The publications related to the security and confidentiality of the data from the electronic file of the patient are analyzed and referenced in the databases Web of Science Core Collection (WoS) and Scopus during the period between 1999 and 2018, incl. The leading countries, scientific institutions, thematic profiles, magazines and authors during this period are highlighted. The scientometric study shows a growing number of publications in recent years and confirms the growing importance of security and data protection when working with the electronic health record.

Specialists developing electronic patient record systems can use the present study and aggregated bibliographic and factual information to find systematic information about the standards that are applied worldwide and their use in different countries and institutions. Young researchers can enrich their theoretical knowledge, which will support their research and future practice.

Study aid

Radkov Rosen, Martin Ivanov Guide for laboratory exercises on „Internet Servers and services". Varna, University Publishing House of TU-Varna. **2021**. 144 стр. ISBN: 978-954-20-0831-6

The guide presents twelve topics for laboratory exercises in the discipline "Internet Servers and Services", studied in the sixth semester by students majoring in "Software and Internet Technologies". A short theoretical presentation is included for each of the topics, after which the specific laboratory statement that needs to be realized and the tasks for implementation are presented. Laboratory exercises can be performed in both face-to-face and non-face-to-face forms of training. To perform the tasks on the laboratory computer, a virtual environment is created in which one or two of the three virtual machines are started and work: Windows server, RouterOS and Asterisk. The results of the implementation of ten of the laboratory exercises are documented in the form of a protocol. As a result of the implementation of the laboratory exercises, students acquire knowledge and develop skills in modern concepts and methods of operation of Internet services (DNS, email, VPN, web, ftp, proxy, VoIP). Knowledge of architecture, operation, configuration and configuration of protocols and services is acquired. Attention is paid to issues related to ensuring optimal configurations and high availability of services.

09.09.2021г   Signature: ……………………………

Varna   / Rosen Radkov, PhD /