UDC 621.391 **doi: 10.26906/SUNZ.2019.5.084**

S. Suhak[1], L. Shabanova-Kushnarenko[2], M. Siruk[3], N. Bihun[4], A. Mishchenko[5]

[1] Military unit A0106, Kyiv, Ukraine
[2] National Technical University "Kharkiv Polytechnic Institute", Kyiv, Ukraine
[3] Military unit A0796, Rivne, Ukraine
[4] Central Research Institute of Weapons and Military Equipment of Armed Forces of Ukraine, Kyiv
[5] Military institute of telecommunications and informatization named after Heroes of Kruty, Kyiv

DATA PROCESSING CENTER AS THE BASIS OF INFORMATION SECURITY OF THE DEFENSE MINISTRY OF UKRAINE

Nowadays, the development of information technologies determines the successful functioning of the political system, since they allow to control political processes, prevent social and political conflicts. Increasing the level of reliability of the information, the most effective use of information resources, external and internal information ropes increase the stability of the political system, stability of the socio-political development of the country. The combination of different telecommunication technologies that create the preconditions for building flexible and high-performance service-oriented systems can be used to solve problems in different industries. However, nowadays, one of the constraints on the implementation and further development of such networks is the theoretical under-development of service delivery models, due to the lack of comprehensive information on the structure of data center networks. During the research conducted by the authors, it was found that the data processing center is the basis for informing the defense ministry of Ukraine. During the research, the authors used general scientific methods of analysis and synthesis, as well as the basic provisions of the theory of informatics, the theory of complex technical systems, the theory of information, etc. During the research, the authors substantiated the main tasks that will be performed by the data processing center of the defense ministry of Ukraine, identified the main information and calculation tasks that will be performed by them. The authors also substantiated the requirements for building a data center of the Defense Ministry of Ukraine. The authors evaluated modern technological solutions and software and hardware for the creation of the information infrastructure of the defense ministry of Ukraine. Possible technical and software for building a reliable and secure data processing center of the defense ministry of Ukraine are proposed. Therefore, the prospective direction of further scientific research of the authors should be considered the justification of ways of improvement of informatization of the armed forces of Ukraine and the creation of information infrastructure of the defense ministry of Ukraine are mobile data centers. This will allow the deployment of information infrastructure in various conditions, including in the open space, which is very relevant for the specifics of actions in the east of Ukraine.

Keywords: informatization, data center, the defense ministry of Ukraine, cloud computing, telecommunication technologies.

Introduction

The proposed information technology, service engineering, and telecommunications systems are іуеештп new pre-projector requests that attempt to create the theoretically unrestricted multiple services that are available. Successful information technology (IT) experience has placed a generator of positive applied active people in various spheres of human life, including in the use of military force and weapons to succeed in military affairs.

In recent years, and in Ukraine, special attention has been given to this issue, so, according to the strategic defense bulletin, the following has been defined: Objective 1.4. Creation of an effective system of operational (combat) command, communication, intelligence and surveillance (C4ISR) ", the end result of which is: creation of a national telecommunication network, modernization and transfer to modern digital technologies of the special communication system, departmental information and communication networks and communication systems for public authorities, as well as the creation of an automated C4ISR component of defense forces that meets NATO standards, doctrines and recommendations, and ensures its integration into NATO system defense management..." [1].

The combination of different telecommunication technologies that create the preconditions for building flexible and high-performance service-oriented systems can be used to solve problems in different industries. However, today, one of the constraints on the implementation and further development of such networks is the theoretical under-development of service delivery models due to the lack of comprehensive data on the structure of the data network center (DNC). Therefore, in the process of providing a composite service, the parameters of the information and telecommunication infrastructure should be taken into account in order to optimally select the elementary components of this service or to migrate it in its virtualized implementation.

The transition to new strategies for implementing public information policy in Ukraine and the use of information in the civilian and military sectors proves that at present our state cannot claim competitiveness without an effective information infrastructure [1-3].

Nowadays, the development of information technologies determines the successful functioning of the political system, since they allow to control political processes, prevent social and political conflicts. Increasing the level of reliability of the information, the most effective use of information resources, external and internal information ropes increase the stability of the political system, stability of the socio-political development of the country.

Therefore, according to the authors, the problem of informatization of the armed forces of Ukraine, one of the directions of which is the creation of the information infrastructure of the defense ministry of Ukraine, is very urgent.

The issue of implementation of information policy and application of modern information technologies in the Armed Forces of Ukraine is a superficially researched question.

Therefore, ***the purpose of the article*** is to evaluate modern technological solutions and software to create a hardware and software platform for the information infrastructure of the defense ministry of Ukraine.

Presentation of the main material

Informatization of the armed forces of Ukraine is a component of informatization of the state and includes the process of creation, implementation and application in different spheres of their activity in peacetime and wartime modern methods, systems and devices of extraction, processing, storage, transmission and use of information. This implies the creation of information infrastructure of the defense ministry of Ukraine, further development of the information and telecommunication network of the armed forces of Ukraine, implementation of the project of the unified automated system in the armed forces of Ukraine [3].

The center of data processing of the Armed Forces of Ukraine should become the software-hardware base and the main component of the information infrastructure of the Ministry of Defense of Ukraine.

A typical DNC structure is shown in Fig. 1.

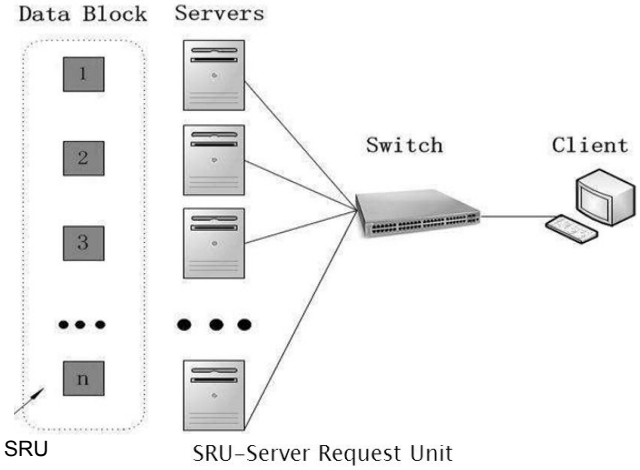

Fig. 1. Typical DNC structure

The main functions of the DNC of the armed forces of Ukraine should be ensured the guaranteed data integrity, continuity of application systems, tasks and services, constant readiness and accessibility of information for users. The tasks of the future DNC of the armed forces of the country are:

- the provision of technological resources in accordance with the growing volume of information being processed;
- ensuring the rapid commissioning of new systems;
- providing guaranteed data retention, backup and data recovery;
- improving the performance of storage systems and their optimization;
- the maintenance of continuity of processes and scalability of information infrastructure.

The approach to creating a data center for the armed forces of Ukraine should be based on the following principles:

- complexity, i.e. to include a complete set of works taking into account the integration of all components into a single information infrastructure;
- multi-vendor, ie each component of the data center can be implemented on the basis of equipment or software of different manufacturers, which will allow to create the optimal solutions in functionality.

The DNC engineering infrastructure is responsible for communications, power supply and cooling and must ensure the smooth and reliable operation of all information systems. The selection of equipment and design of engineering systems is made taking into account the prospects of further development of the DNC, as well as based on the requirements for the level of reliability and availability of information services.

A DNC engineering solution should be aimed to reduce the likelihood of downtime in information systems, which may be due to equipment malfunctions, routine preventive work, or malfunctions caused by personnel errors. The DNC engineering infrastructure has the following components:

- general and uninterruptible power supply systems meeting the requirements for electricity quality and continuity;
- air-conditioning equipment to provide the required values of temperature and humidity in specified ranges throughout the volume of the DNC premises;
- cable system for the creation of reliable physical communication lines of guaranteed quality between the DNC equipment;
- assembly constructions for placement of server and switching equipment of DNC;
- the center floor of the DNC for placement of communication, power cables, pipelines of the system of support of climatic parameters, distribution of cold air, laying of cable lines in the data center premises;
- DNC grounding system for the connection of data center equipment to grounding bus;
- fire extinguishing system.

Table 1 shows possible solutions from various manufacturers for the construction of engineering infrastructure.

Table 1 – **Is the possible solutions from different manufacturers on engineering infrastructure construction**

Comprehensive solution	Rittal, APC, BTICINO
Uninterrupted power supply	Eaton. APC, Neuhaus
Climate control	Stulz, Uniflair, Emicon, Liebert
Mounting constructions 19”	Rittal, Електросила, Conteg
False floor	Uniflair, Jansen

If they approach the critical values, the system promptly informs the dispatcher. Also, the system must implement the function of controlling the work of engineering equipment and provide the ability to automatically prevent the development of emergencies according to the given algorithms [4-6].

The system of monitoring and management of the engineering infrastructure consists of the following components.

Lower level:

- sensors of engineering subsystems of DNC;
- interface converters for gathering information from sensors of engineering subsystems;
- sensors for climate control in server racks in DNC premises;
- current transformers for controlling the parameters of the electricity supply as a whole for the DNC and for each consumer separately.

Intermediate level (automation level):

- a network of programmable logic controllers using open technology and standard protocols.

Top level (level of visualization):

- an automated workplace manager that provides a convenient interface to access the controlled parameters of the data center.

Server hardware is the core of the DNC. The server park should be reasonably productive and redundant, easily managed and scalable, and economical in terms of energy consumption.

Servers, which are dedicated to certain information systems are most often used inefficiently: in the vast majority of cases, their useful load does not exceed 10-15%. Thus, over 70% of the DNC computing capacity is actually idle. To solve this problem, it is advisable to use virtualization technology [2].

Server virtualization allows you to create multiple virtual machines on a separate physical server, each of which solves a separate task.

Thus, multiple virtual servers can run on the same physical server, increasing its aggregate payload. As a result, the degree of server usage can increase up to 70-80%, which will reduce the total number of servers in the DNC and reduce the cost of their acquisition and support.

Data storage systems (DSS) are used to ensure the reliability of storage, high availability and the efficiency of providing large amounts of information. It is advisable to use storage networks to connect DSS to servers, since the direct connection of storage limits scalability and controllability. It is possible to use a multilevel storage model to organize the storage of large amounts of information efficiently. This concept assumes a hierarchical division of information depending on the level of its demand by users [5].

A backup and restore system is a software system that prevents loss of information in the event of equipment malfunction, as well as software or user errors. The backup system must allow the DNC to be stored in full. This guarantees complete recovery of information in the shortest possible time, reduces downtime of the DNC and associated material losses.

Within the DNC project, it is possible to use modern backup systems that support all types of remote copying, mirroring and replication of data (including in real-time) from various sources, using tools for easy copy management in heterogeneous information infrastructure.

Designing and deploying a network infrastructure is one of the most important steps in creating a DNC, as only a properly planned network can provide optimal availability and productivity, the security of its resources, uninterrupted user access and business continuity. The DNC network infrastructure must be implemented through a switched factory that connects the various DNC components: applications, servers, dedicated devices, storage systems and users.

There are four key components to a DNC network architecture:

- a network of high-performance computing to ensure server interaction in high-performance clusters;
- a storage network to consolidate memory resources so that they can be distributed and used more efficiently;
- a network of interconnection with the backup DNC, which connects the main and backup DNC over optical or traditional networks and provides replication and mirroring of data;
- an access network that provides secure access for users.

Uninterrupted operation of all DNC components is not possible without the use of specific physical and information security solutions. DNC physical security systems protect equipment from fire and thermal damage, water and flooding, as well as electromagnetic radiation. In addition, DNC physical security systems prevent the penetration of unauthorized persons and unauthorized access to equipment [2].

In order to protect the information stored and processed in the DNC, it is necessary to use the experience and technologies of leading manufacturers. Decisions must guarantee protection against network attacks, embedded executable code, and unauthorized access to data. This ensures the maximum level of failure of the DNC 1 eliminates the risk of information leakage [4].

The conclusion from the article

The analysis showed that the creation of a single information space is a long and objective process that requires the improvement of forms and methods of information systems management, further centralization and integration of computer databases and the introduction of advanced computer information technologies for the widespread use of effective and powerful computer networks, application of specialized security and information security tools, establishing effective information sharing between users. The authors evaluated modern technological solutions and software and hardware for the creation of information infrastructure of the defense ministry of Ukraine, an integral component of which is the data center.

The article proposes one of the options of hardware and software for building a reliable and secure data processing center of the armed forces of Ukraine. A further direction of the authors' scientific research should be considered in the justification of ways of improving the informatization of the armed forces of Ukraine and the creation of information infrastructure of the defense ministry of Ukraine on the basis of mobile DNC. This will allow the deployment of information infrastructure in different conditions, including in the open space, which is very relevant for the specifics of actions in the east of Ukraine.

REFERENCES

1. Shyshatskiy, A.V., Bashkirov, O.M. and Kostina, O.M (2015). "Development of integrated systems and data for Armed Forces", Arms and military equipment, No 1(5), pp. 35-40. available at : http://journals.uran.ua/index.php/2414-0651/issue/view/1%285%29%202015.
2. Petrushen, M.V(2014). "Evaluation of modern technological solutions and software and hardware for the creation of a data center in the Armed Forces of Ukraine". Control, navigation and communication systems. Poltava: PNTU named after Yuriy Kondratyuk. No 31. pp. 155-160.
3. Minster J. - B., Capitaine N. and Clark D. M(2009). "The new ICSU World Data System: A world-wide community of excellence for data issues". Materials of the Intern. Conf. "Electronic Geophysical Year: State of the Art and Results" / Ed. by V. Nechitailenko, GC RAS, Moscow,117 p. doi:10.2205/2009-REGYconf.
4. Guide to the World Data Center System: General Principles. World Data Centers. Data Services. Paris.: ICSU, 1996. 110 p.
5. Volpe, F(2003). QuickBird High Resolution Satellite Data for Urban Applications. Volpe Fabio, etc. 3 p. http://eurimage.com/products/tech_papers/qb_urban-applications.pdf.
6. Greenberg, A, Hamilton, J, David, Maltz, A. and Patel, P(2009). "The Cost of a Cloud: Research Problems in Data Center Networks". Computer Communication Review. No. 39(1). pp. 68–73.

Рецензент: д-р техн. наук, проф. О. І. Тимочко
Харківський національний університет Повітряних Сил імені Івана Кожедуба
Received (Надійшла) 19.08.2019
Accepted for publication (Прийнята до друку) 25.09.2019

Центр обробки даних як основа інформаційного забезпечення Міністерства оборони України

С. О. Сугак, Л. В. Шабанова-Кушнаренко, М. Г. Сірик, А. О. Міщенко

Сьогодні розробка інформаційних технологій визначає успішне функціонування політичної системи, оскільки вони дозволяють здійснювати контроль над політичними процесами, запобігати соціальним і політичним конфліктам. Підвищення рівня достовірності та надійності інформації, найбільш ефективне використання інформаційних ресурсів, зовнішніх і внутрішніх інформаційних канатів підвищують стійкість політичної системи, стабільність соціально-політичного розвитку країни. Поєднання різних телекомунікаційних технологій, які створюють передумови для побудови гнучких та високопродуктивних сервісноорієнтованих систем, можуть використовуватись для розв`язання задач у різних галузях. Однак, на сьогодні, одним із стримуючих факторів щодо впровадження та подальшого розвитку таких мереж є теоретичне недоопрацювання моделей надання сервісів, що зумовлені відсутністю вичерпних відомостей про структуру мереж центрів оброблення даних. В ході проведеного авторами дослідження встановлено, що основою інформатизації Міністерства оборони України є центр обробки даних, обґрунтовані основні завдання, які їм будуть виконуватися, визначено основні інформаційно-розрахункові задачі. Обґрунтовано вимоги щодо побудови центру обробки даних Міністерства оборони України. Проведена оцінка сучасних технологічних рішень та програмно-апаратних засобів щодо створення інформаційної інфраструктури. Запропоновані можливі технічні та програмно-апаратні засоби для побудови надійного та безпечного центру обробки даних. Перспективним напрямком подальших наукових досліджень авторів слід вважати обґрунтування шляхів удосконалення інформатизації Збройних Сил України та створення інформаційної інфраструктури Міністерства оборони України є мобільні центри обробки даних. Це дозволить розгорнути інформаційну інфраструктуру у різних умовах, у тому числі на відкритому просторі, що є актуальним для специфіки дій на Сході України.

Ключові слова: інформатизація, центр обробки даних, Міністерство оборони України, хмарні обчислення, телекомунікаційні технології.

Центр обработки данных как основа информационного обеспечения Министерства обороны Украины

С. А. Сугак, Л. В. Шабанова-Кушнаренко, Н. Г. Сирык, А. А. Мищенко

Сегодня разработка информационных технологий определяет успешное функционирование политической системы, поскольку они позволяют осуществлять контроль над политическими процессами, предотвращать социальным и политическим конфликтам. Повышение уровня достоверности и надежности информации, наиболее эффективное использование информационных ресурсов, внешних и внутренних информационных канатов повышают устойчивость политической системы, стабильность социально-политического развития страны. Сочетание различных телекоммуникационных технологий, которые создают предпосылки для построения гибких и высокопроизводительных сервисноориентованих систем, могут использоваться для решения задач в различных областях. Однако, на сегодняшний день, одним из сдерживающих факторов по внедрению и дальнейшему развитию таких сетей является теоретическое недоработки моделей предоставления сервисов, обусловленные отсутствием исчерпывающих сведений о структуре сетей центров обработки данных. В ходе проведенного авторами исследования установлено, что основой информатизации Министерства обороны Украины является центр обработки данных обоснованы основные задачи, которые будут им выполняться, определены основные информационно-расчетные задачи. Также авторами обоснованы требования к построению центра обработки данных. Проведена оценка современных технологических решений и программно-аппаратных средств по созданию информационной инфраструктуры. Предложены возможные технические и программно-аппаратные средства для построения надежного и безопасного центра обработки данных Министерства обороны Украины. Перспективным направлением дальнейших научных исследований авторов следует считать обоснование путей совершенствования информатизации Вооруженных Сил Украины и создание информационной инфраструктуры Министерства обороны Украины есть мобильные центры обработки данных. Это позволит развернуть информационную инфраструктуру в различных условиях, в том числе на открытом пространстве, что актуально для специфики действий на Востоке Украины.

Ключевые слова: информатизация, центр обработки данных, Министерство обороны Украины, облачные вычисления, телекоммуникационные технологии.