UDC 004.65 **doi: 10.26906/SUNZ.2023.3.095**

Y. Zhyvylo [1], V. Kuz [2]

[1] National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine
[2] Kruty Heroes Military Institute of Telecommunication and Information Technologies, Kiev, Ukraine

TECHNICAL REQUIREMENTS FOR THE PHYSICAL AND APARTMENT INFRASTRUCTURE OF THE MOBILE DATA PROCESSING AND STORAGE SYSTEM FOR THE DATA PROCESSING CENTRE OF THE CONTAINER TYPE OF FINANCIAL INSTITUTIONS, ENTERPRISES, ORGANISATIONS

Abstract. In modern conditions, the amount of information is constantly increasing, and at the same time, the speed of doing business is increasing. According to Gartner Group estimates, the global average amount of user data per company is 120 terabytes. In turn, according to IDC calculations, last year 35 billion messages were sent in one hour in the world. If these numbers are taken into account, it turns out that one message accounts for approximately 3.4 Мв of information. To be successful, companies not only have to operate with large volumes of data, but also process it quickly and efficiently. At the same time, according to the opinion of the world's leading experts, there are about 40 key macrotechnologies in the world today that determine the level of the economy. These processes were significantly influenced by the specifics of the formation, constant development and transformation of cyberspace. In these areas, breakthrough achievements are predicted, first of all, in artificial intelligence, cloud technologies, internet of things, productivity and nature of computing devices, possibilities of storage, processing and transmission of large arrays of data and information (Big Data), means and technologies for their implementation on radically new principles. The capabilities and vulnerabilities of almost all modern infocommunication and cybernetic systems increasingly depend, in addition, on the growth of the interrelationships of various information systems and control systems among themselves in multiparametric, multidimensional cyberspace and their informational and cybernetic interpenetration, interaction and interdependence, etc. Therefore, taking into account the above, it is necessary to focus primarily on the creation of permanently functioning data processing centers (data centers), and under the conditions of our state's opposition to the aggressor country, to develop appropriate data processing and storage systems on mobile platforms. Another, quite significant and meaningful component is taking into account the modern structures of information protection and cyber security systems, which involve the use of a fairly powerful line of tools, both at the technological and software levels, the use of extensive relevant architectures, protection methods aimed at prejudice, detection and response to potential cyber threats.

Keywords: information, data processing, asset, cyber threats, cyberspace, communication system.

Introduction

Problem statement. The unique capabilities of data centers (DC) guarantee the efficiency and uninterrupted operation of any organization, helping to solve most of the problems inherent in any type of business.

Multicomponent systems provide:

- high reliability of information storage at a fully justified cost;
- significant cost savings due to a variable selection of services and opportunities, which is especially relevant when implementing new IT projects;
- reduction of costs for renting premises, service of equipment and payment of electricity;
- creation of conditions for smooth operation and interaction of the head office and the network of branches;
- the possibility of organizing a reserve office in case of need.

Modern DC allow you to work with a large flow of information, organize centralized data storage, increase the reliability of the entire information infrastructure and ensure communication between the DC and users.

An improperly designed and deployed DC, savings on life support systems: the subsystem of ventilation, air conditioning, fire extinguishing, access control and video surveillance, this can cause negative consequences. Violation of stable functioning or technological processes of DC operation can block access to information, and in the worst case, it will be irretrievably lost. Therefore, it is extremely important for all financial institutions of our country to develop and implement the relevant technical requirements (TR) for data processing and storage systems (DPSS) of container mobile data centers, as well as to ensure the stable operation of the corresponding subsystems in the conditions of the existing risk of violation of banking operations through cyberspace.

Understanding the needs of the present day for conducting business, there is a rather urgent question regarding the creation of an effective and reliable data center (data center), and in the conditions of our country's war, to foresee the development of appropriate the DPSS on mobile platforms. The basis of the implementation of such solutions is the principle of access to corporate network resources and virtualization, which will allow to rationally distribute the load on equipment and ensure uninterrupted operation of applications. The development and implementation of the specified systems (centers) will ensure data storage, backup and data recovery, guaranteed accessibility to all corporate assets. At the same time, the territorial location of data and servers does not matter at all, you can work with data from anywhere, having an access interface and an Internet connection. If necessary, it is possible to organize work from mobile devices.

Kesearch publications. Ensuring the stable functioning of electronic communication systems and

networks of financial institutions of Ukraine in special conditions and ensuring uninterrupted operation of departmental information systems in conditions of martial law, data storage (information), ensuring access to information resources of subjects and users is carried out in accordance to the current legislation of Ukraine, regulatory acts of the National Bank of Ukraine, taking into account international standards, generally accepted international practices and principles [1], in particular:

- Law of Ukraine "On Electronic Communications" (current edition dated 03/31/2023), document 1089-IX;
- Law of Ukraine "On Basic Principles of Ensuring Cyber Security of Ukraine" (Verkhovna Rada Bulletin, 2017, No. 45, Article 403, with amendments), document 2163-VIII;
- Law of Ukraine "On banks and banking activity" (information of the Verkhovna Rada of Ukraine, 2001, No. 5-6, Article 30, with amendments), document 2121-III;
- Law of Ukraine "On Financial Services and State Regulation of Financial Services Markets" (Publications of the Verkhovna Rada of Ukraine (VVR), 2002, No. 1, Article 1), document 2664-III;
- Resolution of the Board of the National Bank of Ukraine dated September 28, 2017 No. 95, document v0095500-17, "On approval of the Regulation on the organization of measures to ensure information security in the banking system of Ukraine" [2];
- National Standard of Ukraine on Information Security DSTU ISO/IEC 27000:2015 "Information Technologies. Protection methods. Information security management system. Overview and dictionary";
- National Standard of Ukraine on Information Security DSTU ISO/IEC 27001:2015 "Information Technologies. Protection methods. Information security management systems. Requirements" [10];
- National Standard of Ukraine on Information Security DSTU ISO/IEC 27002:2015 "Information Technologies. Protection methods. Compendium of practices regarding information security measures";
- Internal Statutes.

The supply of SOZD mobile data center of the container type is carried out on the basis of:

- the Law of Ukraine "On Information" (information of the Verkhovna Rada of Ukraine (VVR), 1992, No. 48, Article 650, with amendments), document 2657-XII [3];
- Law of Ukraine "On the Protection of Information in Information and Communication Systems" (information of the Verkhovna Rada of Ukraine (VVR), 1994, No. 31, Article 286, with amendments), 80/94-VR;
- Law of Ukraine "On Electronic Trust Services" (Verkhovna Rada Bulletin, 2017, No. 45, Article 400, as amended), 2155-VIII;
- Law of Ukraine "On the National Informatization Program" (Adopted on December 1, 2022, entered into force on March 1, 2023), 22807-IX;
- Law of Ukraine "On Protection of Personal Data" (Vedomosti Verkhovna Rada of Ukraine (VVR), 2010, No. 34, Article 481, as amended), 2297-VI.

The above-mentioned regulatory documents and standards provide requirements for the minimum necessary package for the creation, development and use of information systems, networks, resources and information technologies, which are built on the basis of the use of modern computing and communication technology, as well as the creation, implementation, technical support (TS) and improvement of the management system of information security and cyber protection [4].

At the same time, more and more organizations are also realizing that traditional security solutions and manual procedures are no longer sufficient to implement and maintain financial sector security policies. In this context, organizations (institutions, enterprises) are not prohibited from building up their capabilities in matters of information and cyber security. But, taking into account the principles of ensuring information security and cyber protection generally accepted in international practice, financial institutions must manage cyber security risks in their activities, on the objects of the critical information infrastructure of the banking system [5], in accordance with international standards, standards of the European Union and NATO.

The most leading compliance protocols (their releases and components) that financial organizations can no longer ignore are [6]:

1. The Payment Card Industry Data Security Standard (PCI-DSS). A security standard for protecting payment data throughout the payment lifecycle.
2. The Sarbanes-Oxley Act (SOX), the modern database (DB) on "reform of open joint-stock companies and investor protection" and "corporate and audit reporting and responsibility".
3. The Monetary Authority of Singapore-Technology Risk Management (MAS-TRM).
4. General Data Protection Regulation (GDPR).
5. Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) is protection of records and information about clients, the procedure for modernization of cyber security systems of financial institutions.

Therefore, programs, tasks, projects and informatization works aimed at the creation, development, integration and support of information and communication systems, networks, resources and information and communication technologies [7], as well as the fulfillment of security requirements are contained in a wide set of standards regulations, mandates, and guidelines that include PCI-DSS, SOX, and MAS-TRM.

The purpose of the article is to formulate the general technical requirements for the DPSS mobile data center container type of institutions, enterprises and organizations of the financial sector of the state.

The main material

Justifying the purpose of the article, it is proposed to outline the main material of the study according to the following structure:

- general requirements;
- requirements for the DPSS;

- requirements for hyperconverged infrastructure.
- requirements for the hardware platform of the data backup and recovery system.

General requirements (Table 1). The DPSS equipment must be assembled, mounted, configured and tested by the supplier in a container-type mobile data center. The DPSS should work in 24x7x365 mode. The DPSS must be provided with warranty service, technical support and software license updates. The supplier performs design, debugging, maintenance and support of servers and the DPSS exclusively by qualified and certified specialists. All equipment and systems as a whole must comply with current environmental, sanitary, fire and explosion safety standards, as well as other applicable regulatory documents of Ukraine.

Requirements for the DPSS (Table 2). The DPSS must be designed and supplied by a single manufacturer and consist of two subsystems, namely:

• data processing and storage (hyperconverged infrastructure);

• data backup and recovery.

Requirements for hyperconverged infrastructure. The software and hardware complex must be delivered in the form of a hyperconverged infrastructure. That is, the server equipment, data storage subsystems, virtualization environment and control systems of the complex must be supplied in the form of a single integrated physical device (solution) compatible with the existing solution of the financial institution (Dell EMC VxRail AllFlash). The architecture of this solution must be standardized by the manufacturer, described in the documentation and serially produced as a single system.

The manufacturer's technical support service must act as a single point of entry and must not redirect the customer to any other technical support services for software or hardware components included in the solution.

A single monitoring point (single interface) of all hardware and software resources of the complex should be provided. The monitoring system should display all hardware components of the complex in the form of a logical structure.

The monitoring system must support integration with VMware vCenter and display the relationship between certain hardware resources and hypervisors. The monitoring system must ensure the compliance of the installed versions of the manufacturer's microcodes and software, as well as ensure the security settings of all components are checked in accordance with the specified corporate security policies.

The system architecture should eliminate a single point of failure. Servers, network infrastructure, power distribution of all equipment and control systems must be fully duplicated.

Hyperconverged infrastructure should ensure compatibility and automation of network parameters in virtualization environments ESXi (VMware), Hyper-V (Microsoft), Openstack (RedHat, Ubuntu), Docker (Kubernetes) container environment, as well as in the combination of several hardware virtualization platforms within the data center.

Table 1 – **Key characteristics of the solution**

Name	Requirement
hysical parameter	The hyperconverged system must be compatible with a 19" mounting cabinet for server equipment and consist of "server" nodes with processors of the x86 architecture with the possibility of replacing the server without stopping the operation of the entire system. The servers must be equipped with cable organizers for ease of maintenance.
Fault tolerance	Hardware redundancy of power and input/output buses. Each system node must be equipped with hot-swappable power supplies with 1+1 availability level.
Network interface	Each server node must have at least four SFP+10GbE ports and one 1GbE port for management.
Management of a hyper-converged system	A hyperconverged system must be equipped with all the necessary hardware and software tools to implement the following main components: - the provision of a single management interface for all equipment included in the system via the Web. Role restriction of administrator rights; - the control system must be fault-tolerant and be hardware-reserved. Complete failure of the control system should not lead to simple functioning; - the monitoring the performance of the used servers. The possibility of remote installation of software necessary for the operation of the server, including the operating system; - the management at the level of policies integrated with VMware vSphere with the possibility of performance control; - the system should provide management of event logs and analysis of the cause of the incident. The event analytics system must be integrated into the VMware environment.
Data access infrastructure requirements	The data storage subsystem should be based on software-defined data access architecture technologies with the ability to balance load and fault tolerance between all hardware components at the hypervisor core level and use flash drive technologies, deduplication and real-time compression. If it is impossible to implement the subsystem at the hypervisor level, it is necessary to add additional computing resources for virtual machines (VM) that must provide this function. The system must include All Flash disk space based on SSD disks, which can be configured in different levels of data protection: without protection, in a mirror, in a double mirror, in fail-safe groups 3+1 and 4+2 using erasure coding technology, depending on the criticality of the data and use to cache a write operation. Availability of data encryption functionality and "stretched" functionality between cluster data centers. The data storage subsystem must provide logical segmentation of data access at the level of each VM or VM file (a data access failure of one VM should not affect the work of others). It should be possible to assign a protection level to each VM file and set access priorities to disk resources (bandwidth). The data storage system (DSS) must support the creation of a single cluster on the scale of two or more data centers with simultaneous access to data on both resources. The DSS must provide data protection at the level of failure of at least one disk or server node. The system must be able to scale within each node of the cluster and by adding additional nodes. The data storage subsystem should include the possibility of synchronous and asynchronous replication between various systems, both software-defined and classical, based on controllers.

End Table 1

	Appropriate replication software should be provided as part of the solution. The I/O subsystem must support software-defined file access with support for file protocols (SMB, NFS) and management by VMware. Support for data encryption at the datastore and VM level.
Virtualization platform requirements	The platform must support: - operation of the required number of VM users and VM management system and applications; - centralized management of the virtualization platform and automation of administration processes; - load redistribution mechanisms between cluster nodes without stopping VM operation; - mechanisms for changing VM configuration; - provision of mechanisms for snapshots of guest systems; - integration with the VDI control system; - creation of a hierarchical structure of pools of computing resources (CPU/RAM) of physical servers with the assignment of priorities or a dedicated resource reserve; - "hot" addition of processor cores and RAM for a working guest OS; - creation of clones of working VMs with changed network parameters and entry into the MS Active Directory domain.
VMware licenses that must be included in the software and hardware complex	Provide for the availability of VMware vSphere Enterprise Plus, VMware vRealize Operations Advanced licenses for all processors of the software and hardware complex, VMware vCenter Server. software subsystem of software-defined storage, with support for deduplication and compression, and metro cluster for all processors of the software-hardware complex. All licenses must have technical support.
Requirements for a hyperconverged infrastructure server cluster:	
The total number of processor cores in the cluster servers (not including Hyper-Threading or similar technology) is at least 784 cores.	
The architecture and performance of the processor is no worse than Intel CPU GOLD 6348 2.6GHz.	
The total amount of RAM per system is at least 7168 GB.	
The total raw of the disk system is at least 322 TB.	
Server nodes that are mounted in a hyperconverged infrastructure	
Processor per node is at least two Intel Xeon Gold 6348 2.6G, 28C/56T processors or equivalent.	
The memory per node is 512 GB, memory slots are at least 32 GB. The possibility of increasing the amount of RAM at least up to 4 TB.	
Storage devices per node	At least two 400GB NVMe drives, U2 G4, Intel Optane P5800X (or similar) and support for the "hot" replacement function. At least six 3.84TB SSD drives, 2.5" with parameters no worse than 1DWPD and support for the function of "hot" replacement. The possibility of installing at least 24 drives of 2.5" (SAS/SATA/NVMe) and 4 drives of 2.5" HDDs (SAS/SATA). The node supports a disk space of at least 184 TB.
Boot disks are 2x M.2 SATA 480GB RAID1 with support for the "hot" replacement function.	
Power supply units are at least 2x 1400W 250v with C13-C14 cables connected to the PDU.	
Connecting to an Ethernet network switch per node	At least 4 10/25 Gbps Ethernet Opt SFP28 ports, without using PCIe expansion slot. At least 4 optical modules SFP+ SR Optic, 10GbE. At least 4 optical cables OM3/4 LC/LC Fiber Cable 5 meters long. Expandable by adding additional PCIe NICs.
Management requirements	The server must have software and hardware from the server manufacturer for configuring management and monitoring the operation of all components.
Management mechanism in conditions of lack of physical access to them	Graphical interface/Remote power management/Platform independent text or graphical console for displaying remote server activity management/Command ribbon and scripting interface/SSL encryption. Ability to diagnose CPU and server. DNS\DHCP support. Ability to update IPMI microcode via local network. Ability to connect images as local disk devices.
Support for hypervisors and virtualization management environments VMware® ESXi 7.0U3	
Technical support	- at least 36 months of warranty and service support from the equipment manufacturer; - support must be provided 24*7*365; - the response time to a service request is no later than 4 hours from the moment the request is received by the service department; - warranty support should include replacement of failed components, access to software updates and support from the technical support center of the equipment manufacturer; - service, if necessary, is carried out at the location of the equipment; - availability of a single call center of the equipment manufacturer for receiving service requests.
Implementation requirements	- physical installation of equipment on site according to specifications; - installation of OS, drivers, embedded software, software for virtualization, hypervisors, cluster manager and SupportAssist agent; - deployment and configuration of the system in accordance with the requirements described in the manufacturer's documentation; - sending configuration data to the technical support service.

Table 2 – **Requirements for the DPSS equipment located in a separate segregated area**

№	Equipment name	Unit	No.	Technical and quality requirements
1	Server	pcs.	2	Number of central processors: 2 pcs.; Central processor: at least 32 cores; RAM: at least 512 Gb; Hard Drive: No worse than 10K RPM SAS 12Gbps 2.5in Hot-plug; Total capacity of hard drives: at least 18 TB; Type of supported disks: SATA/SAS; Size and maximum number of HDD slots: 8x2.5; Number of Gigabit Ethernet ports: 2; Chassis type: Rack; Number of power supply units: 2 pcs.; Power, W: 1000.
2	Server	pcs.	4	Number of central processors: 2 pcs.; Central processor: at least 16 cores; RAM: at least 64 Gb; Hard Drive: No worse than 10K RPM SAS 12Gbps 2.5in Hot-plug; Total capacity of hard drives: at least 12 TB; Type of supported disks: SATA/SAS; Size and maximum number of HDD slots: 8x2.5; Number of Gigabit Ethernet ports: 2; Chassis type: Rack; Number of power supply units: 2 pcs.; Power, W: 1000.

Backup and recovery system hardware platform requirements. The software and hardware complex of data backup and recovery should be delivered as an extension of the existing solution with the possibility of data replication from different sites where the equipment is located. The hardware part of the complex (Table 3) must support:

• data invulnerability architecture, which ensures data integrity throughout the entire life cycle;

• an architecture that allows you to reduce the load on the disk subsystem due to the transfer of all data processing processes to the processor and RAM;

• technology that allows for the transfer of only unique data from the PC server or client to the system, and also provides the ability to manage data replication between similar systems;

• use of segments of variable length, which improves the level of deduplication and compression;

• real-time deduplication immediately after the backup flow enters the system and save only unique elements to the disk;

• high recovery speed, process parallelism, verification and recovery of data integrity [9].

Table 3 – **Hardware part of the complex**

Name	Requirement
Control module	With high-speed deduplication function at the level of variable-sized blocks without the process of buffering non-deduplicated data on disks. Write cache must be duplicated on non-volatile memory. The system must withstand power outages without a UPS and resume operation after extended periods without power.
Software	The system management software should work on the controller of the storage system, without the need to allocate an additional server for this task [10]. GUI over Web, command line interface over SSH protocol must be supported. Support for command scripts.
Scale requirements (no less)	The system must provide copy speeds of at least 15 TB/h for transfer protocols (CIFS, NFS, VTL) and at least 30 TB/h for protocols with a distributed deduplication function. Address the physical capacity of 280 TB of usable space, including hot-swap drives and RAID redundancy [10].
Storage devices	60 discs 4TB or more 7.2K NL-SAS. The system must support hot-swappable disks that are used system-wide. Their number should not be less than the number of disk shelves of the system.
Data protection	RAID-6 and support for checking data integrity using content hash
Connection ports	At least 4 10 Gbps Base-T ports and 8 10 Gbps Ethernet SFP+ ports. At least 8 optical cables OM3/4 LC/LC Fiber Cable 5 meters long.
Support of the main functionality	The deduplication technology should ensure the global exclusion of duplicated blocks and their recording in a single storage pool, regardless of the use of protocols, the type and number of virtual devices, and the type of data storage. The deduplication technology should provide functionality expansion by transferring part of the load to the server of the backup system using protocols compatible with OST. The system must support the function of end-to-end data integrity, including checking the correctness of recorded data in real time. The system must provide a constant background check of data integrity, with the condition that each block must be checked at least once a month. The system must be available 24/7 for backup and recovery. Service procedures should be launched no more than once a week and should not block basic functionality. The system must provide support for a synthetic full copy of the data. The system must have High Availability configuration settings at the controller level. In the absence of such an opportunity, provide for the storage of additional copies of data on a separate system with technical characteristics, licenses and service support similar to the main system.
Support of the additional functionality	Availability of WORM functionality (Retention Lock) of images and data encryption. The system must support the mechanism of quotas and logical isolation of data, which limits the logical volume of backup copies and access to them. The system must provide remote distributed replication of data (replication must be performed over IP channels and must provide simultaneous deduplication: only unique (non-deduplicated) blocks of data from media servers and OS agents must be replicated. The system must support extended functionality for data replication under the control and on demand of backup software using OST-compatible protocols. A replication bandwidth control mechanism must be provided. Support for two-way authentication of users and quotas for folders and all network access protocols. Support for role-based administration of backups and the system as a whole. Support for filtering access by IP and DNS name. Support for encryption of backup and replication traffic.
Support for data access protocols using IP CIFS, NFS, VTL, OST, NDMP without the use of additional devices.	
Support for caching on SSD	To cache metadata and ensure a full start of the VM with backup. The presence of a separately installed hardware adapter responsible for data compression. Availability of at least 2 SSD drives with a volume of at least 3.84TB each for caching.
Monitoring	Statistics of occupied space by customers, auto generation of service requests.
Licensing and service support	- the system must have all necessary licenses to fulfill the above requirements; - all licenses without exception must be given in possession; - technical support for all equipment for a period of 36 months with a service level of 8*5, a response to a service request within the next working day; the system must support installation in a standard rack; - if it is necessary for the organization of the normal functioning of the system or the implementation of system management involving other software products, such as an OS or a database, then all necessary licenses for additional software products must be included in the offer. The term of technical support for such components should not be less than the term of technical support for the disk system for saving backup and archive copies.

The software part of the complex must be from the same manufacturer as the hardware part, and be integrated into a single system or be an extension of the "Veeam" backup platform available to the Customer.

The software part of the complex (Table 4) should provide:

1. Centralized backup and recovery operations for complete control of data protection across multiple computing and storage environments.

- virtual and physical environments;
- critical business applications;
- data storage networks (SAN) [8], network attached storage (NAS) and direct attached storage (DAS);
- backup storage options, including tape drives and libraries, virtual tape libraries, disk arrays, deduplication storage systems, and cloud object storage.

2. Virtual synthetic full backup.

3. Starting the VM directly from backup.

4. Data replication, namely local, remote and parallel-local and remote with continuous data protection for recovery at any point in time.

5. Management of several software products from one console.

6. Monitoring and analysis and search capabilities.

7. Authorized project administrators, developers and users to order new IT services and manage certain cloud and IT resources based on their roles and privileges.

Table 4 – **The software part of the complex**

System software functionality for data backup and recovery	- Backup system management support via WEB, GUI and CLI. - Support for VMware and Microsoft Hyper-V virtual infrastructure hypervisors. - Availability of clients for Windows and Linux OS (Cent OS, Debian, Fedora, Oracle Linux, Red Hat, Suse, Ubuntu). - Availability of clients for UNIX systems (AIX, Solaris, HP-UX). - Availability of agents for the following application systems and databases: Exchange, SharePoint, MS SQL, SAP IQ, SAP, SAP HANA, Domino, Oracle, IBM DB2, Informix, Sybase ASE. - Consistent database backup with distributed deduplication and integration with native backup tools. - Availability of backup indexing tools and data search organization for all created backups. - Support for authentication when working with backup storage devices. - Support for encryption of backups and data when transferred to the backup device. - Provision of reading and writing data directly from clients to the backup storage device with the storage of service information on the backup server. - Providing integration with the backup storage platform using data transfer optimization protocols, support for distributed deduplication and creation of virtual (synthetic) full copies. - Support for VM startup technologies directly from the secure backup storage platform, providing simultaneous writing and reading from the secure platform. - Provision of advanced backup and recovery capabilities of VMware virtual environments, such as: changed block tracking technology (CBT), instant access to VMs, granular recovery of objects. To minimize backup and recovery time, the use of modified block tracking technology is mandatory for both backup and recovery. - Ensuring the possibility of continuous data protection for VMware workloads by performing synchronous or close to it (RPO no more than 1 min.) VM replication. Continuous protection of VMware workloads should provide the ability to protect both individual VMs and simultaneous protection of selected VMs collected in protection groups and provide the ability to restore the operation of VMs to any selected recovery point within 24 hours. - Provision of automatic collection and analysis of monitoring data and reporting.
System software performance	- Providing multi-threaded backup and recovery. - Support for multiplexing data streams when creating backups. - Support for dynamic allocation of file system backup tasks to several threads. - Support for deduplication at the source (before transmission over the network to the backup storage device) with recognition of repeating blocks and support for identification of variable length blocks.
Reliability and integrity of information	- The software should perform automatic protection of the stored backup directory, provide the possibility of their further recovery, and also be able to notify in case of finding errors in the backup. - Provision of integral backup of application programs and databases. - Support for restoring interrupted backup sessions from a known integrity point.
Integration with other management interfaces	- The solution should provide extensions that allow integration with own management interfaces: VMware vRealize Automation, VMware vCenter, System Center. - Integration with vSphere with the ability to manage backup and restore operations from the virtual environment management console. - Support for data exchange via REST API with other systems.
Software Licensing, Warranty and Deployment	- Licensing type is per active physical processors (CPU/sockets) or per volume of data to be backed up (FETB). - The minimum number of required licenses are 28 sockets or 160 FETB. - All licenses without exception must be given in possession. - Technical support for a period of 3 years with a service level of 8*5, a response to a service request the next working day. - Provide opportunities to use all types of agents for the OS, databases and application servers listed in the software functionality requirements. - The granted licenses must ensure the protection of productive data, application programs and databases without any restrictions: both functionally and in terms of the number of objects. - Backup system components and/or additional management servers must support Windows or Linux deployment. - If the installation of any components of the backup system requires the involvement of other software products, such as an OS or a database, then all necessary licenses for additional software products must be included in the offer. The term of technical support for such components must not be less than the term of technical support for the backup software. - If for the normal functioning of the software it is necessary to install additional components that may require separate hardware resources (for example, servers performing data deduplication), such hardware resources must be included in the offer, with a technical support term no less than the technical support term for the backup software.

If the supplier already has a modern backup platform “Veeam” installed and functioning with extensive security and security functions, as well as the ability to access data from anywhere in the world [11], then the company can put forward additional technical requirements for the IT infrastructure, services and equipment, this is Table 5.

Conclusions

Summarizing what has been said, it should be noted that today corporations and institutions of the global financial market process and store a fairly powerful array of confidential data, such as customer transactions, account information and private personal data of payment cards, payment processors, etc.

Modernization of the structures and topologies of electronic communication systems and networks of financial institutions is influenced by the development of technologies, changes in the financial security environment, forms, methods and technologies of using cyber influence and new achievements in this. At the same time, this circumstance is complicated by the constant change in the volume, speed and variety of attacks, which vary from denial of service to malicious theft from the inside.

Table 5 – **Additional technical requirements for IT infrastructure, services and equipment**

Functionality of the backup platform	The backup platform must have a distributed and horizontally scalable backup architecture, have the ability to back up itself to restore settings, provide a Rest API for remote configuration and management, and ensure the use of a central management server as a license distribution server. Backup of VM. The backup platform should provide the ability to back up VMs at the image level, with the ability to copy only changed blocks and save the state of applications, as well as without installing specialized applications inside the VM. The backup platform must support backup transfer, both over the transmission network and over the storage network, including backing up VMs directly from NFS storage. The backup platform must support a mechanism for automatically changing the speed of the backup process when the read response time increases at all levels of the storage system with the ability to define response time thresholds. The backup platform should have deduplication and compression mechanism of backup, the ability to exclude blocks of OS service files, as well as folders and files specified by the user, to speed up the backup process, as well as to reduce the amount of data storage. The backup platform must be able to use DSS hardware snapshots for backup, with the ability to ensure application integrity within the VM. Interaction should be implemented using specialized APIs at the storage level and without installing additional software on them. Testing the integrity and ability to restore VM backups. The backup platform should be able to create an isolated environment for the customer's production infrastructure, with the ability to use it for automatic backup testing or to create test zones. The backup platform should be able to automatically test the functionality of the backup of the VM. Verification should be performed by running associated backup VMs and/or DSS hardware snapshots in an isolated environment on a schedule, with the ability to test the performance of applications and services inside the reserved VMs. It should be possible to use both built-in verification scripts and the ability to use custom scripts. Backup of network resources. Provide the ability to create a backup copy of network resources to which public access is provided via SMB (including SMB v3) or NFS (including NFS v4.1) protocols. Support the ability to create VSS snapshots when backing up data using the SMB v3 protocol to ensure consistency. Have the functionality of storing historical versions of files, with the possibility of downloading the oldest versions to a secondary backup storage. Support the ability to use DSS hardware snapshots as a backup source for file resources, avoiding file locking limitations. Interaction should be implemented using specialized APIs at the storage level and without installing additional software on them [12]. Storage of backup of VM. The backup platform must integrate with specialized backup storage solutions (deduplication disk storage device): EMC DataDomain via DDBoost protocol, HPE StoreOnce via Catalyst protocol, as well as Quantum DXi, ExaGrid and Fujitsu. A backup platform should be able to encrypt backups. The backup platform must be able to integrate with Linux-based machines to use them as secure backup repositories, allowing data immutability settings to be set to protect against deletion and modification of backup data blocks for a specified period of time. The backup platform must be able to combine different physical DSS into a logically single scalable backup storage pool, to combine the available space of individual DSS. A backup platform must be able to transfer backups between different repositories with the ability to specify a new storage depth for the backup. When transferring backup copies between repositories, the backup copy platform must be able to restore transfer of backup copies between sites using compression mechanisms and global deduplication of traffic, and hashing of information at both sites on specialized servers. The backup platform must support backup to tape libraries, including multi-streaming, the ability to pool tape drives from different tape libraries. The backup platform must be able to create a synthetic full back up when writing to tape from backups available in the disk storage of an incremental full backup cycle, without creating a temporary synthetic full copy on disk. Possibilities of replication and disaster recovery of VM. The backup platform should support direct VM replication for Microsoft Hyper-V and VMware vSphere platforms, without using intermediate backups, with the ability to ensure the creation of multiple recovery points and the transfer of only changed blocks. The platform must ensure the integrity of applications inside the VM during replication, without installing specialized applications inside the VM. When replicating VMs between repositories, the backup platform must be able to restore replicas between sites using compression mechanisms and global deduplication of traffic, and hashing information on both sites on specialized servers. The backup platform must provide switching to the replicated VM with the possibility of automatic IP address change. The backup platform must provide failover to a VM that is replicated even if the backup server is lost. Continuous replication and disaster recovery for VMware vSphere VMs. The backup platform must support continuous replication of VMware vSphere VMs, without using virtualization snapshots, which ensures minimal data loss within 2 seconds. The platform must continuously replicate the I/O operations of the VM and store them in a special log on the target datastore for several hours specified in the short-term storage policy, in order to ensure the possibility of restoring the VM to a certain point in time with a given step. The platform should provide the possibility of creating additional control points of VM recovery, which go beyond the short-term replication policy, taking into account the state of those working inside the application and ensuring their consistency, without installing specialized applications inside the VM.
Support of virtual infrastructures	Support for backup of virtual infrastructure based on the VMware vSphere 5.5 and higher platform, including VMware vSphere 7.0 U1, availability of VMware Ready for vSAN certification. Support for copying virtual infrastructure based on the Microsoft Hyper-V platform starting from Windows Server 2008 R2 SP1 and higher, including Microsoft Hyper-V 2019 and support for 64 TB VHDX. Support for backing up vApp containers, VMs and their metadata, as well as restoring them directly to the vCloud Director infrastructure. Support for automating tasks and ensuring the ability to work through the self-service portal for VMware vCloud Director.
Integration with other management interfaces	The solution should provide extensions that allow integration with its own management interfaces: VMware vRealize Automation, VMware vCenter, System Center. Support for data exchange via REST API with other systems.
Software Licensing, Warranty and Deployment	Requirements for technical support and updating the backup system. 1st level technical support should be available in multiple languages. Technical support should include the possibility of updating to new versions of the basic software. Technical support must be provided 24 hours a day, 7 days a week, 365 days a year. General requirements for the supply of software. The license should not have any technical and functional restrictions, as well as restrictions on the further increase in the number of protected environments. The supplier must have official partner status from the software manufacturer. The supplier must provide an official authorization letter from the manufacturer confirming the possibility of supplying the software as part of the procurement procedure. The supplier must provide a license certificate for the software.

The creation of permanently functioning data centers is a guarantee of business stability in the conditions of martial law. Their implementation will ensure data storage, backup and recovery, guaranteed accessibility to all corporate assets. Therefore, taking into account the technical requirements for data processing and storage systems of container-type mobile data processing centers of institutions, enterprises and organizations of the financial sector of the state is a requirement of today.

REFERENCES

1. Platform for effective regulation/Ministry of Economy of Ukraine, About banks and banking activity, [Electronic resource]. – Access mode: https://regulation.gov.ua/documents/id147305.
2. Aidina Olha Heorhiivna, State registration of normative legal acts as one of the means of protecting the rights of citizens, [Electronic resource]. – Access mode: https://minjust.gov.ua/m/str_5948.
3. The Cabinet of Ministers registered a draft law on the protection of technological information, [Electronic resource]. – Access mode: https://cedem.org.ua/news/kabmin-zareyestruvav-zakonoproekt-pro-zahyst-tehnologichnoyi-informatsiyi/.
4. Resolution of the Board of the National Bank of Ukraine dated September 28, 2017 No. 95 "On approval of the Regulation on the organization of measures to ensure information security in the banking system of Ukraine", (document v0095500-17), [Electronic resource]. – Access mode: https://bank.gov.ua/ua/legislation/Resolution_28092017_95.
5. Order of the Administration of the State Service of Special Communications and Information Protection of Ukraine dated January 15, 2021, No. 23 "On Approval of Methodological Recommendations for the Categorization of Critical Infrastructure Objects" (document v0023519-21), [Electronic resource]. – Access mode: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text.
6. Strategy for the development of the financial sector of Ukraine until 2025, [Electronic resource]. – Access mode: https://bank.gov.ua/ua/about/develop-strategy.
7. Law of Ukraine "On the National Informatization Program" (document 2807-IX), [Electronic resource]. – Access mode: http://ru.osvita.ua/legislation/law/3163/.
8. Data storage and processing systems, [Electronic resource]. – Access mode: https://www.pronet.ua/sistemi-zberigannya-i-obrobki-danikh/.
9. Order of the Ministry of Finance of Ukraine dated October 5, 2004 No. 630 "On approval of the conceptual architecture of the information and analytical system of the Ministry of Finance of Ukraine" (document v0630201-04), [Electronic resource]. – Access mode: https://zakon.rada.gov.ua/rada/show/v0630201-04#Text.
10. DK 021:2015 code 48820000-2 "Servers" (Server equipment as part of a data storage system for the development of the system of public services of the Dnipropetrovsk Regional State Administration for the fulfillment of clauses 2.2 and 4.4 of the tasks of the regional informatization program "Elektronna Dnipropetrovsk" for 2017 -2019 years), [Electronic resource]. – Access mode: https://prozorro.gov.ua/tender/UA-2018-09-07-000361-a.
11. How to manage IT infrastructure remotely: settings, data protection, search for vulnerabilities and other nuances, [Electronic resource]. – Access mode: https://itc.ua/ua/articles/yak-keruvati-it-infrastrukturoyu-viddaleno-nalashtuvannya-zahist-danih-poshuk-vrazlivostej-ta-inshi-nyuansi/.
12. Technical requirements and quality criteria of the subject of procurement, [Electronic resource]. – Access mode: https://dniprorada.gov.ua/upload/editor/tehnichne_zavdannya.doc.

Received (Надійшла) 16.07.2023
Accepted for publication (Прийнята до друку) 06.09.2023

Технічні вимоги до фізичної та апаратної інфраструктури системи обробки і зберігання даних мобільного центру обробки даних контейнерного типу фінустанов, підприємств, організацій

Є. О. Живило, В. С. Кузь

Анотація. В сучасних умовах обсяг інформації постійно збільшується, і при цьому швидкість ведення бізнесу - збільшується. Згідно з оцінкою Gartner Group, середньосвітовий обсяг призначених для користувача даних, що припадає на одну компанію, становить 120 терабайт. У свою чергу, за розрахунками IDC, в минулому році за одну годину в світі відправлялося 35 млрд. повідомлень. Якщо враховувати ці числа, то виходить, що на одне повідомлення припадає приблизно 3,4 Мб інформації. При цьому, за думкою провідних світових експертів сьогодні в світі існує біля 40 ключових макротехнологій, які визначають рівень економіки. Визначним чином на ці процеси вплинули особливості формування, постійний розвиток і трансформація кіберпростору. В цих сферах прогнозуються проривні досягнення перш за все у штучному інтелекті, хмарних технологіях, інтернет-речах, продуктивності та природі обчислювальних засобів, можливостях зберігання обробки та передачі великих масивів даних та інформації (Big Data), засобах і технологіях їх реалізації на кардинально нових принципах. Можливості і вразливості практично всіх сучасних інфокомунікаційних та кібернетичних систем все більше залежать, крім того, від зростання взаємозв'язків різноманітних інформаційних систем і систем управління між собою в багатопараметричному, багатовимірному кіберпросторі та їх інформаційно-кібернетичного взаємопроникнення, взаємодії і взаємозалежності, тощо. Тому, враховуючи зазначене першочергово необхідно зосередити увагу на створенні стало-функціонуючих центрів обробки даних (дата-центрів), а за умов протистояння нашої держави країні-агресору розробити відповідні системи обробки та зберігання даних на мобільних платформах. Іншою, доволі суттєвою та змістовною складовою є врахування сучасних структур систем захисту інформації та кібербезпеки, які передбачають застосування доволі потужної лінійки інструментів, як на технологічному так і на програмному рівнях, використання розгалужених відповідних архітектур, методів захисту які спрямовані на упередження, виявлення та реагування на потенційні кіберзагрози.

Ключові слова: інформація, обробка даних, актив, кіберзагрози, кіберпростір, комунікаційна система.