UDC 621.391

FEATURES OF THE CLOUD SERVICES IMPLEMENTATION IN THE NATIONAL NETWORK SEGMENT OF UKRAINE

Mykhailo M. Klymash, Ivan V. Demydov, Mykola I. Beshley, Olga M. Shpur

Lviv Polytechnic National University, Ukraine

Background. Cloud computing environments and services on their basis offering unprecedented cost savings, improved exchange of information and the efficiency of the infrastructure. Accordingly, by using these solutions we can increase the efficiency of the national network services segment. Thus the scalable service architecture development of network systems is a key aspect which directly forms the preferred national electronic services, both public and private sectors.

Objective. The aim of the paper is to find the ways of optimal consolidation of cloud service systems for the timely transformation of single national information space Ukraine. According to the authors, providing an opportunity to influence these processes by government oversight agencies is critical to Ukraine

Methods. Relevance of research in this area is confirmed by the rapid development of commercial technologies that make cloud implementation process simpler, safer and much more productive on the criteria of transparency, integration, expansion (scalability), quality of service. The introduction of cloud services by public and private operators of distributed service platforms requires consolidation of needs for cloud service technologies, and the harmonization of tariffs for their use by public oversight bodies such as NCCIR of Ukraine. Obviously, the developers of cloud service solutions must have the tools available to maintain service availability and quality, based on the technical and target parameters.

Results. Proposed architectural features of the cloud services implementation technologies, including private cloud using existing structures to support the government and civil service systems at significantly reducing capital expenditures, provided support to the required level of security.

Conclusions. Creation of a common cloud service network information environment requires data-centered model (in the long term DaaS), which has trusted data processing center based core, provided with the decent level of protection and functionality, spreading a corresponding policy on all joint data processing centers of national segment cloud network system by means of interoperability, which allows to deliver services demanded here and now, using replication and migration of corresponding services and link data (including inter-operator and cross-platform).

Key words: cloud-system, cloud computing, virtual machine, cloud structure, government and public service system..

Introduction

In modern socio political and economic circumstances, taking network and information technologies development into the account, a problematic of ubiquitous computing deployment comes to prominence, which aims at lowering computing resources consummation while solving a wider range of data processing tasks in terms of required distributed services providence. With all respect to government’s compliance monitoring agency’s significance in network transformation process, it’s worth noticing that the reduction of budgetary funding demands the revision of service infrastructure creation and modification approaches with the purpose of it’s effectiveness and security enhancement, especially within the bounds of national network segment [1]. The result of these transformations appears to be the Joint Information Environment, as end user location independent, service independent, reliable and robust quick data access and computing access environment.

The global experience shows that cloud platforms and services allow service applications to achieve more opportunities for rapid evolution of service applications in all branches of national economy of Ukraine, including diversified oversubscription of service applications and their components by various government and non-government organizations. The specialized research directions in this context of utilization, besides cyber security, are Information assurance [2], which includes data integrity protection, data and corresponding informational services accessibility, authentication tasks and user data confidentiality. Apparently, such methods require physical, technical and administrative means. This methodological aspect refers to the data being transmitted, as well as stored data. The important topics are also system adaptability insurance [3], operational continuity (independent service availability level), functional ability, service implementation effectiveness, data and services migration management, overcoming the bondage to access networks, which, in particular, is the tactical objective of modern wireless access technologies. Customer service in a discontinuous connection mode is also an interesting subject.

To overcome the outlined challenges telecom and infocomm providers (service operators) should unite their efforts by consolidating their data centers and design agencies under the auspices of government authorities, which, as a result, leads towards the elaboration of common cloud technologies deployment policies, another words, creating a relevant methodology according to industrial or general social problems. These arrangements allow to avoid the deployment if inefficient calculating and network capacities.

An experience of American government organizations [4] militates that if some number of data processing centers in the cloud system are assigned as core, it's functionality can be spread apart a different part of the system, stepwise changing it's architecture, service components and optimizing corresponding internal data exchange processes, which will enhance interoperability of elementary service applications inside data processing centers and interoperability of the whole network system in general. Aside from that, such an approach allows to separate service application models and data transmission models by information types according to the required information security level: unprotected data (Non-secure Internet Protocol Router Network), protected data based on corresponding secure transmission protocols (Secure Internet Protocol Router Network) and restricted access information, which pertains additional protective measures (Top Secret Sensitive Compartmentalized Information) within dedicated network infrastructure [5].

In our opinion, the main condition of cloud technologies implementation in national service network infrastructure segment is coordination of service components distributed utilization policy for multiple service providers in terms of quality, security and service availability criteria. Accordingly, it is possible to define the following set of cloud system adaptation measures in national service network infrastructure:

1. The initial implementation of cloud services: defining the strategy and paths of effective development, user base, fields of application (government and commercial services, e-government in particular);
2. Optimal consolidation of national data processing centers: virtualization and consolidation of data and application service components;
3. Implementation of consolidated national cloud network infrastructure: integration of multi operator environment within data processing center consolidation, distributed services providing optimization through the created infrastructure as part of service components distributed utilization policy, constant updates of service and technological system components;
4. Cloud service delivery effectiveness enhancement: delegation of authorities about service components maintenance to third party operators, commercial services support, expansion of offered services list and amounts of provided service instances, control from supervisory authorities (NCCIR of Ukraine).

A goal of this research is the search of optimal consolidation paths for the opportune transformation of common national information space of Ukraine. On the authors' opinion, involving government supervisory authorities' influence on these processes has the critical significance for Ukraine.

General concepts of cloud technologies based transformation of service network systems of Ukraine

Implementations of cloud technologies anticipate providing the most innovative, effective and secure informational and infocomm services to ensure transparent deployment of ubiquitous computing in national network segment with the appropriate control of government supervisor authorities.

According to National Institute of Standards and Technology (NIST) definition, cloud computing is the model of unspecialized on-demand network access to a pool of configured computing resources. These resources are: networks, servers, storage systems, applications and services. A common taxonomy of models, which are used to implement and deliver cloud services (Fig. 1) includes three general concepts: Software as a Service (SaaS), Platform as a Service (PaaS), and also Infrastructure as a Service (IaaS) [6]

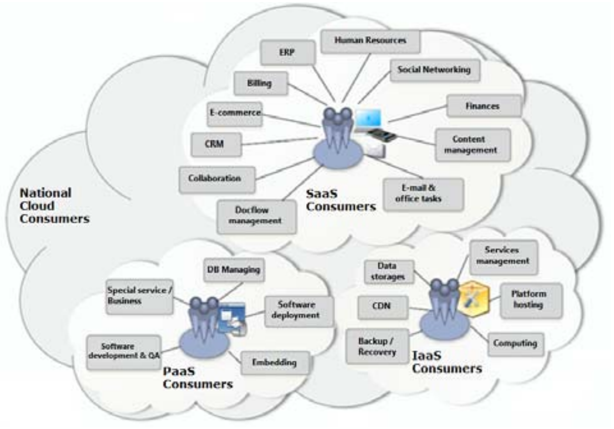

Fig. 1. An example of services available to the cloud users

A common feature of these models is focusing on provisioning (supporting and delivering) informational technologies as a service, which is delivered to users by service providers. Traditionally, the latter conduct IP-based interaction. Government supervising authorities' efforts should be directed to propagation of cloud technologies for their successful utilization by national users and formulating a sustainable interest to attract investments into current industry from government, as well as commercial organizations.

Main benefits of cloud computing (effectiveness, performance, innovations) are listed in table 1.

Summing up the above, it can be stated that:

- cloud systems consolidation is one of the key problems, which leads to saving service users' capital investments, lowers operational cost of ineffectively distributed and cumbersome service delivery platforms. Further, almost "instant" scalability of modern cloud solutions allows to deliver customers the exact needed amount of services here and now, which becomes an actual subject of financing when necessary. How effective is the management of service network solutions, the greater the economic feasibility of implementing cloud technologies, including software development for new cloud applications;
- rapid global access to critically important information in high availability circumstances and optimal redundancy of cloud "ubiquitous computing" allows for greater resistibility of service network infrastructure to different crisis situations, maintaining continuity of system operation;
- lowering user information broadcast time in constant scaling circumstances can be achieved by parallelizing collection, processing and storing large amounts of data in joint cloud network systems, which cannot be implemented using other approaches in modern infocomm industry;

- Table1

Main benefits of cloud computing implementation

Effectiveness	**Performance**	**Innovations**
Basic means utilization – server computing capacities around 60-75% (existing systems – less than 30%)	Receiving service from trusted infocomm providers here and now (no need for lingering expensive infrastructure construction)	Shifting accents from basic means management to service management (management approach modernization)
Advanced level of demands aggregation, accelerated cloud systems consolidation (existing systems tend to inhere server capacity duplication, separated request flows)	Almost instant growth and decrease of service network systems performance (unlike traditional approaches, which take lot more time)	Industrial and organizational culture level increase
Application development and implementation productivity increase, network, terminal and software management improvement (unlike existing systems)	More rapid response speed to modern demands of national industry government and private sectors (for example, IoT implementation)	(government management reforming, data flows management effectiveness increase, electronic government)

- cloud technologies allow for network services delivery constant monitoring by government supervising authorities, yet questions about effective security of national network segment still remain;
- an additional benefit from cloud technologies implementation is unification of services access based on simplification of legal entities and individuals' identification in a common national level authentication system;
- mutual association of network and computing power and system data processing center consolidation leads to reducing of systemic inhomogeneities in operational points of presence and, as a result, reduced heterogeneity of cloud systems.

Five main categories of organizational and technical problems occur during cloud based transformation of Ukrainian service network systems, which are::

1. Management culture transformation. Setting a supervising control by the public authorities of Ukraine for cloud technology implementation escort within national segment of service network systems: defining the key entities, their authorities, events list, including educational nature.
2. Ensuring functional withstandability, information delivery insurance and security. Implementation of a security policy in terms of real time competent authorities control over cloud services, which will allow detection of network attacks, unauthorized intervention, perform a system diagnostics and proper counteraction to detected threats. This task raises a topic about working out an official document that characterizes national security policy in field of cloud service platforms. Critically important network infrastructure segments protection also gains significance, which is mainly determined by hardware containing objects secrecy level, as well as authorized personnel access methods (card-based, two-factor identification and so on) and internal cloud storage.
3. Overcoming the "last mile" tactical network dependency. Delivering network services in capacity, regulated by access network bandwidth, taking a possibility of performing some operations without guaranteed connection into the account, and also in discontinuous network connections circumstances.
4. Service purchasing and overcoming financial difficulties. Cloud infrastructure financing for service delivery under pay for demanded amount of services principle. Data processing center core formation in order to create and broadcast service components for the purpose of saving time and money on introduction of new services and more flexible management of the latter. A refusal of financing of underloaded and unproductive network service components should be provided. Contract based operator B2B and G2B interaction to provide integrity and migration of data in cloud environment
5. Data and services migration, functional transparency. In order to solve this task information presentation variability should be provided in order to support multiple service platforms, which will allow modern approaches to processing and analyzing data collected by legal interception also. The use of common standards for data transfer, as well as legal compliance, including legislation which is associated with personal data protection [7].

Phases of cloud technologies implementation in national segment of service network infrastructure

It is obvious that any transformation in complex systems is not instantaneous. Transformation of network environment towards cloud service delivery platform formation is no exception. The transfer of network infrastructure to infocomm providers' field of responsibility is and effective decision, that draws software responsible personnel's attention to certified software products development for modified network environment and not to hardware operating. National segment cloud network environment (Fig. 2) is a solid base for ubiquitous computing concept support in different branches of national economy of Ukraine, as well as building protected institutional infocomm systems, subject to the uniform implementation of standardized requirements for carrier equipment.

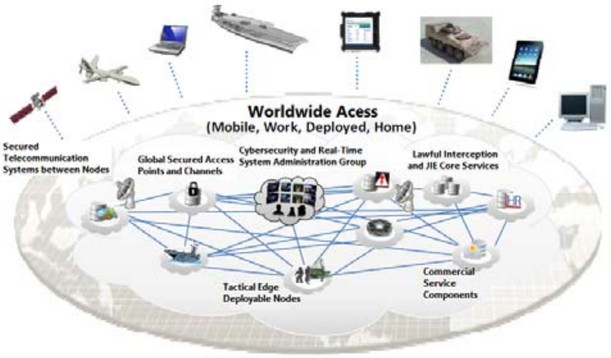
Worldwide Acess
(Mobile, Work, Deployed, Home)
Secured Telecommunication Systems between Nodes
Global Secured Access Points and Channels
Cybersecurity and Real-Time System Administration Group
Lawful Interception and JIE Core Services
Tactical Edge Deployable Nodes
Commercial Service Components

Fig. 2. Cloud environment of national service network segment

This environment (Fig. 2) contains grid infrastructure analogue, which combines control and security components, commercial computing platforms and operators' points of presence, partners' networks and government authorities' networks.

Let us take a closer look at cloud infrastructure implementation stages, which were partially mentioned above:

1. The initial implementation of cloud services: determining the government strategy, management structure and effective evolution paths, user base analysis and expansion, determining fields of application (government and commercial services, e-government in particular).

The main difficulty in national level cloud environment implementation is the necessity of defining government authorities' field of responsibility, as well as key figures, who control the national service system implementation processes, interdepartmental interaction and have enough authority to perform a professional activity in development and implementation of relevant regulations field. Accountability of these figures should be regulated by NCCIR regulations. A change of traditional service delivery paradigm appears necessary, which will bring innovative society and organizations interaction technologies, take the specifics of their activity into the account to maximize the system emergence during business processes, which are becoming more unified, integrated and coordinated in data-centered network environment. Stimulating common network environment usage for cloud computing model implementation will lower the organizations' needs in specific support and dedicated specialists, especially from system administering field.

A scientific reasoning of the required system performance or system capacity is an important topic, which will have a direct impact on the necessary amount of investments, a type of alternative system edition, it's architecture, a complex of service components and service amount of infocomm operator service platform.

Therefore, firstly, the technical maintenance cost is reduced, which is transferred to infocomm providers under the contract bases; secondly, replaced by funding basic tools for distributed computing funding generated by consumption and the provision of relevant information and communication services in the cloud network infrastructure; thirdly, using a single cloud environment is the need for new approaches to contact and budgeting, leading to substantial savings and investment is more responsive, implementing the "pay for what you consumed" principle.

Thereby, we initiated research in problems relating to both the three branches of science: technical (prevails), government management and economic.

Interesting are: sociological aspect, which refers to direct consumption of infocomm services by interested figures and groups, as well as methodological aspect of training specialists for management positions to be a matter for the relevant competencies assessment efficiency and planning of the cloud environment by the aforementioned general criteria.

2. Optimal consolidation of national data processing centers based on standardized software platforms and cloud environment core data centers group, which simplifies national system segment administration, allows corresponding virtualization and consolidation of data and application service components; also, potential intrusions plane is reduced, network attacks plane in particular.

Cloud environment implementation strategy in a national network segment involves placing key service components and data in the data processing center core to protect them and control the relevant information flows. This allows to not only reduce the load on redundant peripheral computing resources, but also to increase utilization coefficient of involved software, interoperability of software platforms in case of their constant monitoring by operative system administration division. Standardization of service provision in different data centers to optimize internal business processes of their operation in general. As a result – higher data processing center performance, lower network attacks possibilities due to improvement of management processes. Preference should be given to the centralization of data centers in protected sites, as opposed to the development of peripheral computing power. During the development of new applications or their migration to newly created data processing centers, network environment properties will allow applications to migrate in groups using the so called "linked" data, which will follow the carriers wherever they are needed. This approach also makes effective operational activities in the informational space possible. A "virtual desktop" concept drastically increases passing existing resources to new user groups, who make use of common cloud infrastructure informational environment, unbound from its tactical parameters and geographical location.

3. Implementation of consolidated national cloud network infrastructure: integration of multioperator environment under data processing centers consolidation, distributed services delivery optimization through the created under distributed services components appliance policy.

High adaptiveness to destructive influences [8] is a well-known advantage of cloud environments, since hardware or functional failure of one or a few nodes makes almost no effect on resistibility and functionality of cloud system. Simultaneously, the possibility of the whole system being in inoperable state is rather low. Data and applications security in a common informational environment are inversely proportional dependent to cloud systems' complexity, and thus directly proportional to consolidation and standardization level of software and hardware means of distributed services delivery platforms. Core data processing centers of common cloud environment info space require IaaS, SaaS, PaaS layers' functions and cashing functions (virtual content replication). Under such conditions the system will have a high scalability (both software and computing). This scalability in the transition from traditional to cloud service infrastructure (Fig. 3) is vital in terms of the maintenance of basic services and their related information flows under the control of supervisory authorities and to continuously improve them for software and technological level, which greatly affects on systems' resource consumption system.

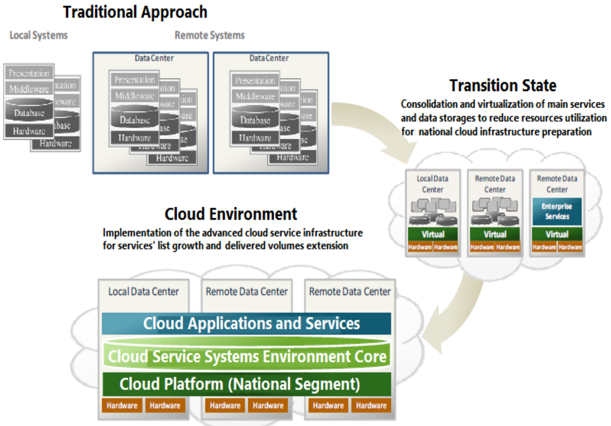
Traditional Approach
Local Systems
Remote Systems
Data Center
Data Center
Presentation
Middleware
Database
Hardware
Transition State
Consolidation and virtualization of main services and data storages to reduce resources utilization for national cloud infrastructure preparation
Local Data Center
Remote Data Center
Remote Data Center
Enterprise Services
Virtual
Hardware
Cloud Environment
Implementation of the advanced cloud service infrastructure for services' list growth and delivered volumes extension
Local Data Center
Remote Data Center
Remote Data Center
Cloud Applications and Services
Cloud Service Systems Environment Core
Cloud Platform (National Segment)
Hardware

Fig. 3. Consolidated data processing centers forming the base of common cloud informational platform national segment

Supervising authorities can take part in load distribution of cloud platform, service list formation and delivery control, as well as their compliance with the information redundancy demands, particularly in terms of it's security, transmission and storage reliability. Such monitoring should be constant, which will allow rapidly reacting to potential cyber threats [1].

It is also worth focusing should also focus on the data-centric aspects of the cloud infrastructure formation. By means of standardization of data formats of presentation she global cloud platform developer community determines that two main categories of electronic services should be delivered: operational services and informational services. Functionally, operational services are IaaS, SaaS, PaaS in informational process technological support context. To informational services NIST professionals include SaaS and PaaS layer functions. It is also worth mentioning DaaS (Data-as-a-Service) concept, which regards to processing the so called big data and granting access to cloud metadata. Here a comment about traditional network data storages would be in order. They currently can't handle the amount of information traversing from no-SQL cloud solutions DaaS (Google's Big Table, Apache's Hadoop/HBase, Erlang Mnesia etc.). And it is not only because of the large amounts of unstructured data or weakly structured information, which is hard to process with traditional instruments. The thing is within unprecedented scalability and performance of cloud solutions, which leads to the new quality of such systems – cross-cloud functional transparency. This apparently is due to the increase of standardization, stability and functionality of appropriate software and hardware, independently of their purpose, which, in long terms, allows for inter-cloud application exchange based on environments compatibility.

4. Cloud service delivery efficiency improvement: process of outputting service components to third-party operators, commercial services support, expanding offered network services list and their amount, supervising authorities control (NCCIR of Ukraine).

Regulatory authorities' efforts in cloud technologies implementation field in Ukraine should be directed to solving the following problems:

- support of centralized management and functional transparency for all national segment cloud systems of service network infrastructure;
- promote the final transfer of «triple play» services to the IP platform;
- the implementation and expansion of services for the identification of electronic services users in Ukraine.

Aside to this, authors seems appropriate to briefly describe the risks, which accompany the latest transformations in information and telecommunication space of the country. It is clear that cyber-attacks on network systems today are often very well-planned and aggressive. So, naturally, we should determine that the commercial use, which are operated independently infocomm operators, the first stage must work with information, which is accompanied by low risk, as in case of loss or diversion, it will not have a material adverse effect on the functioning of the respective entities.

On the other hand, if the information is critical, its protection will require special software and hardware, which in turn will use a certain amount of cloud computing power.

Conclusions

1. Creating a cloud environment in the national segment of the network infrastructure service is a fundamental aspect of the further strategic development of Ukraine's information space.

2. A prerequisite for the effective development of electronic services is a set of organizational measures aimed at consolidating hardware and software to create scalable cloud computing power for systems based on heterogeneous multi-operator platform that includes high functional transparency.

3. Creation of a common cloud service network information environment requires data-centered model (in the long term DaaS), which has trusted data processing center based core, provided with the decent level of protection and functionality, spreading a corresponding policy on all joint data processing centers of national segment cloud network system by means of interoperability, which allows to deliver services demanded here and now, using replication and migration of corresponding services and link data (including inter-operator and cross-platform).

4. Cloud infrastructure requires continuous monitoring, swift system administering, and its evolution – an effective government supervision of public authority, such as NCCIR (National Commission for the State Regulation of Communications and Informatization).

5. Third party infocomm operators' services should be used for higher scalability of cloud network system, which allows to quickly build up the necessary computing power according to current needs, however requires accurate record management of governing and regulative documents.

6. Evaluation and effectiveness parameters leveraging methods of scalable cloud service systems require further research. Similarly, consideration of novel infocomm technologies is indispensable, which allow system architecture to adapt to wider range of services in secure national service network infrastructure segment, involving IoT concept in particular.

References

1. Demydov I., Concept of the migrating firewall to scalable cloud networks / Ivan Demydov, Orest Lavriv, Zenoviy Kharkhalis, Mohamed Mehdi El Hatri // Modern problems of radio engineering, telecommunications, and computer science Proceedings of the International Conference TCSET'2016 (Lviv-Slavske, Ukraine February 23 – 26, 2016) – Lviv: Publishing House of Lviv Polytechnic, - 2016, - P.643-645.
2. https://en.wikipedia.org/wiki/Information_assurance
3. Strykhaliuk B. M. Structural and functional synthesis of heterogeneous service-oriented telecommunications networks: Abstract dissertation for the degree of doctor of technical sciences 05.12.02 - Telecommunication systems and networks / Bogdan M. Strykhaliuk; Ministry of Education and Science of Ukraine, National University "Lviv Polytechnic". - Lviv, 2015. – 40 P.
4. Federal Cloud Computing Strategy, Feb 2011 // www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf
5. DoD Cloud Computing Strategy // www.defense.gov/Releases/Release.aspx?ReleaseID=15435
6. NIST Special Publications: [SP 500-292] NIST Cloud Computing Reference Architecture, September 8, 2011
7. DoD Directive 4630.5 Interoperability of IT and NSS, May 5, 2004 // www.dtic.mil/whs/directives/corres/pdf/463005p.pdf
8. Demydov I. V. The structural-functional synthesis of cloud service delivery platform after service availability and performance criteria / I. V. Demydov, B. M. Strykhalyuk, O. M. Shpur, Mohamed Mehdi El Hatri, Y. V. Klymash // Information processing system. — 2015. — № 1. — P. 144-159.

Received in final form on March 25, 2016

Климаш М.М., Демидов І.В., Бешлей М.І., Шпур О.М.

Особливості впровадження хмарних сервісних систем в національному мережному сегменті України

Проблематика. Хмарні обчислювальні середовища та сервіси на їх основі пропонують безпрецедентну економію коштів, вдосконалений обмін інформацією та ефективність функціонування інфраструктури. Відповідно, використання таких рішень дозволяє підвищити ефективність сервісів національного мережного сегменту. Таким чином, розроблення архітектури масштабованих сервісних мережних систем є ключовим аспектом, який безпосередньо формуватиме перевагу національних електронних сервісів, як державного, так і приватного секторів.

Мета. Метою даного дослідження є пошук шляхів оптимальної консолідації хмарних сервісних систем для своєчасних трансформацій єдиного національного інформаційного простору України. На думку авторів, забезпечення можливостей впливу на дані процеси з боку державних наглядових структур є критично важливим для України.

Методи. Актуальність досліджень у даному напрямі підтверджується швидким розвитком і синтезом комерційних технологій, які роблять процес впровадження хмарних систем простішим, безпечнішим, а також значно продуктивнішим за критеріями прозорості, інтегрованості, розширення (масштабованості), якості сервісу. Впровадження хмарних сервісів державними та приватними операторами розподілених сервісних платформ потребує консолідації потреб у хмарних сервісних технологіях, а також узгодження тарифів на їх використання державними наглядовими органами, наприклад НКРЗІ України. Очевидно, що розробники хмарних сервісних рішень повинні мати у розпорядженні інструментарій для підтримування оптимальної сервісної доступності та якості, базуючись на необхідних технічних та цільових критеріях.

Результати. Запропоновано архітектурні особливості реалізації хмарних сервісних технологій, які, зокрема, використовують існуючі приватні хмарні структури, для підтримки урядових та державних сервісних систем при значному зниженні рівня капітальних затрат, за умов підтримки необхідного рівня безпеки.

Висновки. Ефективне створення єдиного інформаційного середовища (JIE) хмарної сервісної мережної системи передбачає дата-центричну модель (в перспективі DaaS) , яка містить ядро на основі довірених ЦОД, котрі володіють необхідним рівнем захищеності та функціональності, поширюючи відповідну політику на всі консолідовані ЦОД різних операторів хмарної мережної системи в рамках національного сегменту за рахунок інтероперабельності, яка дозволяє надавати послуги в обсягах, що необхідні саме тут і зараз, шляхом реплікації та міграції відповідних сервісів і пов’язаних даних (в тому числі міжоператорської та крос-платформенної).

Ключові слова: cloud-система, хмарні обчислення, віртуальна машина, хмарна структура, урядові та державні сервісні системи.

Климаш М.Н., Демидов И.В., Бешлей Н.И., Шпур О.Н.

Особенности внедрения облачных сервисных систем в национальном сетевом сегменте Украины

Проблематика. Облачные вычислительные среды и сервисы на их основе предлагают беспрецедентную экономию средств, усовершенствованный обмен информацией и эффективность функционирования инфраструктуры. Соответственно, использование таких решений позволяет повысить эффективность сервисов национального сетевого сегмента. Таким образом, разработка архитектуры масштабируемых сервисных сетевых систем является ключевым аспектом, который непосредственно будет формировать предпочтение национальных электронных сервисов, как государственного, так и частного секторов.

Цель. Целью данного исследования является поиск путей оптимальной консолидации облачных сервисных систем для своевременной трансформации единого национального информационного пространства Украины. По мнению авторов, обеспечение возможностей влияния на эти процессы со стороны государственных надзорных структур является критически важным для Украины.

Методы. Актуальность исследований в данном направлении подтверждается быстрым развитием и синтезом коммерческих технологий, которые делают процесс внедрения облачных систем проще, безопаснее, а также значительно более продуктивным по критериям прозрачности, интегрированности, расширения (масштабируемости), качества сервиса. Внедрение облачных сервисов государственными и частными операторами распределенных сервисных платформ требует консолидации потребностей в облачных сервисных технологиях, а также согласование тарифов на их использование государственными надзорными органами, например НКРСИ Украины. Очевидно, что разработчики облачных сервисных решений должны иметь в распоряжении инструментарий для поддержания оптимальной сервисной доступности и качества, основываясь на необходимых технических и целевых условиях.

Результаты. Предложены архитектурные особенности реализации облачных сервисных технологий, которые, в частности, используют существующие частные облачные структуры, для поддержки правительственных и государственных сервисных систем при значительном снижении уровня капитальных затрат, в условиях поддержания необходимого уровня безопасности.

Выводы. Эффективное создание единой информационной среды (JIE) облачной сервисной сетевой системы предусматривает дата-центрическую модель (в перспективе DaaS), которая содержит ядро на основе доверенных ЦОД, которые обладают необходимым уровнем защищенности и функциональности, распространяя соответствующую политику на все консолидированные ЦОД различных операторов облачной сетевой системы в рамках национального сегмента за счет интероперабельности, которая позволяет предоставлять услуги в объемах, которые необходимы именно здесь и сейчас, путем репликации и миграции соответствующих сервисов и связанных данных (в том числе межоператорской и кросс-платформенной).

Ключевые слова: cloud-система, облачные вычисления, виртуальная машина, облачная структура, правительственные и государственные сервисные системы.