INFORMATION AND WEB TECHNOLOGIES

DOI 10.51582/interconf.21-22.05.2021.029

Bekmagambetova Gulmira
PhD., Associate Professor,
Kokshetau A. Myrzakhmetov University, Republic of Kazakhstan

INFORMATION TECHNOLOGIES IN THE SPHERE OF CLOUD TECHNOLOGIES

Abstract. *This article discusses the protection of information when using information technologies in the field of cloud computing. What methods are used to build protection in cloud computing and how it is implemented.*

Keywords*: cloud technologies, cloud computing, information security, “Cloud”.*

Introduction.

Over the past five to seven years, a new trend has emerged in the information technology industry-cloud computing. Although “Cloud computing” is just a method of providing computing resources, and not a new technology, they have launched a new branch of development in the system of providing information and services.

Initially, information technology was dominated by large computing machines. Over time, this system gave way to a client - server model. The modern industry of information technology is becoming more mobile, more productive and, of course, more focused on providing services. But this update, like any other update, contains the old components from which it was “born”.

Main part.

Security problems in the information technology system are global in nature, and they are of great importance for the entire information technology ecosystem. Now it is necessary to understand that without using global information space, Kazakhstan expects an economic downturn. Kazakhstan's participation in international information exchange systems is impossible without solving the problems of data security in the information and communication sphere. Timely access to information and computing resources supported by the Internet is, of course, a good thing. But, you need to understand that the Internet as a Global network can serve both for good and for harm. This is mainly due to the problems of ensuring the security of information resources. This problem is particularly acute now for Kazakhstan, since the country's own infrastructure is not yet ready for full protection, an example is the recent DDoS attack on a large hosting provider in Kazakhstan, which penetrated many enterprises, but the country's leadership is working in this direction. As an example, we can mention the introduction of a security certificate for state and quasi-state enterprises, the organization of a "State Technical Service" to respond to incidents related to information security.

With the growth of technological progress, there are certain opportunities for improvement and losses associated with the protection of information. It is no secret that in our time, cloud technologies are an integral part of society.

This article will discuss the protection of information when using information technologies in the field of cloud computing. Information security is carried out under the condition of ensuring its confidentiality, availability and integrity by applying various methods such as the creation and improvement of an information security system, the development, use and improvement of information security tools, the creation of systems and means to prevent unauthorized access to the processed information, as well as the identification of technical methods that pose a threat to the normal functioning of IT systems.

In connection with the growth of possible losses from the insecurity of information resources, it pushes us to look for new ways to improve the effectiveness of information protection. When using or providing access to information resources, you must follow the following methods:

– data storage encryption;

– protection when transmitting data over public networks using a virtual private network (VPN) and cryptographic transmission protocols such as SSL (Secure Sockets Layer), TLS (transport layer security);

– use of authentication when accessing systems – it is also possible to use two-factor authentication using email or SMS;

– implementation of distributed file systems like Ceph, GlusterFS, Amazon S3.

One of the urgent directions of increasing the productivity of using information systems can be the use of “Cloud computing”. It should be noted that the exact translation of the term “Cloud computing” does not quite accurately reveal modern systems for servicing remote users. Cloud computing, in addition to remote execution of applications, provides a full range of information services, including storage, retrieval and transmission of information, ensuring its security and other like that.

Cloud computing is very popular now. Cost-effectiveness, simplicity, multi-user architecture-contributes to the popularity, and also assumes all the possibilities of information services, including storage, search and transfer of information, ensuring its security, and much more.

Cloud technologies (or cloud computing) are technologies for distributed processing of digital data, with the help of which information resources are provided to the user as a service. The programs are launched and display the results of their work in a browser window on a personal computer. At the same time, all applications necessary for operation and their data are located on a remote Internet server and are temporarily cached on the client side: on personal computers, game consoles, laptops, smartphones. The advantage of the technology is that the user has access to his own data, but does not have to worry about the infrastructure, operating system and software with which he works. The word “Cloud” is a metaphor for a complex infrastructure that hides all the technical details.

Cloud computing technologies are aimed at solving the following problems:

– Convenient work with files on several gadgets: editing and processing them without transferring from one device to another, without having to worry about software compatibility. Solving the problem of limited space on the hard disk of a computer or flash drives;

– Issue of licensed software;

– The ability to simultaneously work on one document for several people.

"Cloud" is now called everything, so you need to decide on the terms. A cloud is a model that provides on-demand access to a specific shared pool of configurable computing resources. Depending on the cloud model, various services can be provided:

– VPS/VDS (Virtual Private / Dedicated Server - virtual machine rental),

– VDI (Virtual Desktop Infrastructure - virtual desktop rental),

– web application hosting rental,

– SaaS (Software as a Service - application rental),

– IaaS (Infrastructure as a Service - infrastructure rental),

– DaaS (Desktop as a Service - another marketing name for VDI),

– BaaS (Backup as a Service-rental of backup infrastructure).

In fact, all this diversity comes down to renting virtual machines with certain nuances of access and installed software.

The main properties of cloud computing are:

– scalability (scalable application provides more load by increasing the number of running instances);

– elasticity (allows you to quickly increase the capacity of the infrastructure by adding new compute nodes and new software);

– multitenancy (reduces cloud platform costs and uses available computing resources);

– usage fee (transfer of part of capital costs to operating costs);

– self-service (allows consumers to request and receive the required resources in minutes).

Cloud technologies and the services they provide can be paralleled with utilities. In both hot and cold weather, water and electricity consumption varies, so the consumption of services provided by "Cloud" platforms can increase or decrease depending on the increase or decrease in load.

One of the main advantages of "Cloud technologies" is security, if properly provided.

There are several fundamental cloud services on which the entire service delivery system is built as a cloud.

Currently, 3 types of deployment are used:

– Private;

– Public;

– Hybrid.

Private clouds are designed for internal corporate use. Such computing resources can be located both on the enterprise site (own data center) and on the side of the cloud service provider, while access is closed from outside, providing the first echelon of security. This model provides a high degree of control and a high degree of security due to the fact that the infrastructure and users are within a secure perimeter. The system will be built in such a way that productivity and efficiency are at a high level. But you need to understand that this deployment model incurs material costs for equipment and labor. An organization that has taken this path must make a large financial contribution to the IT infrastructure by purchasing hardware and software, and paying for information technology specialists.

Public clouds are very common these days. The service is provided by cloud service providers, unlike a private cloud, it provides services to a wide range of users. These include Google Drive, Microsoft OnDrive, Dropbox, and so on. This infrastructure is located on the side of the cloud provider, and has a number of advantages. Among them, it can be noted - the absence of capital expenditures for the purchase of hardware and software. The model can also be beneficial to those enterprises where the risks of service downtime can have a very negative impact on the business, since the service of a cloud provider is serviced by qualified personnel and has very powerful equipment compared to private ones. One of the disadvantages of this approach is the lack of control by the user, the provision of low performance, data transfer rates and a weak security system.

Hybrid “Clouds” combine the infrastructures of the above models. Providers provide some of the services as a private “Cloud”, and some as a public one. This combination allows you to save on organizing your own infrastructure, but at the same time gain control and a high level of security.

And so, to properly understand cloud computing, you need to remember that they, in fact, inherit from their predecessors. In this amazing new world of cloud computing, there is room for an innovative combination of cloud technologies and the proven performance of legacy systems such as powerful mainframes. This approach provides information technology staff with a huge opportunity to control changes and use them for the benefit of themselves and their organization.

Cloud computing represents a significant advance in the development of information technologies and services. By providing on-demand access to shared computing resources in an offline, dynamically scalable, and calibrated mode, cloud computing offers clear advantages in speed, agility, and information efficiency. In this technology, security plays an important role; Specialists pay special attention to this problem. But, despite all the difficulties in the field of security, the advantages of services provided via the Internet outweigh the possible risks and “Cloud technologies” will be widely in demand in the information technology market for a long time.

Conclusions.

Thus, information security is a very serious problem for humanity. Today, we often process, store or transmit data that is subject to regulatory and regulatory requirements. If your data is subject to regulatory or regulatory restrictions, choosing a cloud deployment (private, hybrid, or public) depends on understanding whether the provider fully complies with these requirements. Otherwise, there is a risk of violating confidential, regulatory and other legal requirements. When it comes to privacy, information security matters are important.

From the above, we can conclude that security is not always provided only by protection. This can also be achieved by the appropriate rules of behavior and interaction of objects, high professional training of personnel, reliable operation of equipment, reliability of all types of ensuring the functioning of information security objects. Confidentiality of information is the principle of audit, which states that auditors are obliged to ensure the safety of documents received or prepared by them in the course of their audit activities, and do not have the right to transfer these documents or their copies to other persons.

References:

1. Malyuk A. A., Ozhered I. V. Prospects for the development of "cloud" technologies. Information security and protection of personal data in the cloud // Bulletin of the National research nuclear University "MEPhI", Moscow, 2013. No. 1. P. 120-124.

2. URL: JSC "STATE TECHNICAL SERVICE" (sts.kz), regulations of JSC "STATE TECHNICAL SERVICE" (sts.kz).
3. Fundamentals of information security. Textbook for universities / E. E. Belov, V. P. Los, R. V. Meshcheryakov, A. A. Shelupanov. - Moscow: Hotline-Telecom, 2006.
4. A. E. Kononyuk. Fundamental theory of cloud technologies. Kiev, 2018.
5. Bagrov E. V. Monitoring and audit of information security at the enterprise. Bulletin of the Volgograd State University. Volgograd: 2011, p. 56.