Cloud standards.

There are various organizations that lead the development of cloud standards. The Open Cloud Consortium (OCC) is engaged in the development of standards in the field of cloud computing and their compatibility.

Standards in the field of cloud security (ISO / IES JNC 1 / SC 27).

Standards in the field of cloud security (Cloud Security Alliance).

Development of cloud standards reflecting the interests of cloud computing users (Cloud Standards Customer Council).

Standards in the field of interoperability and practical implementation of cloud systems (IEEE,).

Definition of cloud computing: requirements for the use of cloud computing in the public sector National Institute of Standards and Technology (NIST),

Update of WS, SAML, XACML standards. KMIR in connection with the spread of cloud computing (OASIS,).

Cloud Data Management Interface (CDMI) specification, Storage Networking Industry Association (SNIA) www.snia.org/cloud

The main properties of cloud technologies.

The National Institute of Standards and Technology NIST (National Institute of Standards and Technology. USA) in its document "The NIST Definition of Cloud Computing" defines the following characteristics of clouds:

- the possibility of automated self-service of the system on the part of the provider at a high7 level;

- availability of the Broad Network Access system;

- concentration of resources on separate sites for their effective distribution;

- fast scalability (resources can be allocated indefinitely and released at a higher speed depending on needs);

- managed service (the cloud management system automatically monitors and optimizes the allocation of resources).

Combining resources into pools (Resource pooling). The computing resources of the provider are combined into pools to serve many consumers according to the multi-tenant model. Pools include various physical and virtual resources that can be dynamically assigned and reassigned according to consumer requests. It is not necessary for the consumer to know the exact location of the resources, but it is possible to specify their location at a higher level of abstraction (for example, country, region, or data center). Examples of this kind of resources can be storage systems, computing power, memory, network bandwidth.

Instant elasticity (Rapid elasticity). Resources can be easily allocated and released, in some cases automatically, for rapid scaling proportional to demand. For the consumer, the possibilities of providing resources are seen as unlimited, that is, they can be assigned in any amount and at any time.

Measured service. Cloud systems automatically manage and optimize resources with the help of measurement tools implemented at the level of abstraction in relation to different kinds of services (for example, management of external storage, processing, bandwidth or active user sessions). Used resources can be tracked and controlled, which provides transparency for both the provider and the consumer using the service.

Open-source cloud platforms.

As the competition in the cloud market grows, the cloud service becomes more and more open. Closed source texts are one of the risks associated with cloud computing. For example, if a cloud provider starts dictating unacceptable terms to users, then users have nowhere to go.

Such risks are higher compared to the risks of using closed source software. For example, having legally purchased software can be used even after the supplier changes its terms or goes bankrupt. When using cloud services, users do not have this option.

Also, cloud services work on uncontrolled computers and therefore extremely limit the possibilities of studying the program in operation and reverse engineering in order to ensure COMPATIBILITY.

Also, user data is stored on remote servers, which requires a high level of trust in the provider.

Open-source cloud platforms can solve some problems.

For example, having source texts, you can organize a service that is compatible with the reference one. Market competitiveness also increases, which eliminates the possibility of arbitrariness on the part of the monopolist. In principle, the openness of the source texts makes it possible to deploy cloud solutions in the company's own infrastructure as well: if at some point it turns out that the use of third-party servers is associated with excessive risks, then the open code allows you to transfer applications to your own controlled platform with minimal costs.

The first form of open-source cloud platform that was commercially successful is the Eucalyptus (USA) IaaS system. In the summer of 2010, the OpenStack project was launched. There are other IaaS systems: Cloud Stack, OpenNebula. All mentioned platforms belong to the IaaS segment.

In the field of PaaS systems, open source was not popular until recently, until VMware provided its Cloud Foundry project. With Cloud Foundry, developers will be able to develop scalable applications in one of the popular development systems (frameworks) of their choice, including Spring, Ruby on Rails and Node.js, transferring applications from platform to platform. According to the announced data. Cloud Foundry can work both on infrastructure from VMware itself, and on the Amazon Web Services cloud platform, or even on a developer's personal computer.

Private cloud is not always implemented by the customer. A private cloud means privacy, not a specific location, resource ownership, or self-management. Many providers offer non-local private clouds, that is, allocate resources to a single customer, eliminating the sharing of the same pool by several customers. "The cloud is called private because of its privacy. and not by where it is deployed, who owns it and is responsible for managing it." Some, for example, can place their data centers with hosting providers or pool the resources of different customers, but isolate them from each other using a virtual private network (VPN) and other similar technologies.

Private cloud (as well as public cloud) is not only infrastructure services. Server virtualization is a big trend and therefore a powerful engine of private cloud computing. But private cloud isn't just about infrastructure as a service (laaS). For example, for the development and testing of new software. A high-level platform as a service (PaaS) makes more sense than just providing virtual machines.

Today, the fastest growing segment of cloud computing is laaS. It provides the most low-level data center resources in an easy-to-use form, but does not fundamentally change the principles of work. To create new cloud-first applications and prioritize completely new services that may be very different from what previous applications provided, developers are more comfortable using PaaS.

A private cloud can stop being private. On the one hand, the private cloud has the advantages of the cloud: the speed of reconstruction, scalability and efficiency, eliminates some of the security threats, potential and real, that are characteristic of public clouds. On the other hand, over time, the level of service, security and compliance control in public cloud services will definitely increase. Therefore, some private clouds may well move into the category of public clouds. Most of the private cloud services, most likely. will evolve into hybrid cloud services, expanding available opportunities through the use of publicly available cloud services and other third-party resources.

Fog computing.

Fog computing is a technology thanks to which data storage and processing takes place in a local network between the end device and the data center. "Fog", unlike "cloud", is closer to users. This is a decentralized system that filters information entering the data center.

Advantages:

• Offloading from the cloud. The use of fog technologies together with cloud technologies helps to reduce the load on the data center. Local servers process data and send only the most important ones to the data center.

• Data transmission in real time. "Fog" is closer to the user, so the time for processing and transmitting information is reduced.

• Additional security. In the local network, there is another level of protection - a virtual firewall, traffic segmentation or something else.

Disadvantages:

• Problems with network nodes. Decentralized networks are less reliable than networks of large data centers.

Scope of use.

Fog computing is used to connect Internet of Things (IoT) devices. With the help of "fog", data is transmitted and analyzed almost without delays, which is critical for some IoT devices - for example, sensors in self-driving cars.

Simply put, fuzzy computing is sharpened under machine-to-machine interaction.

Machine-to-machine interaction (M2M) is a technology related to the Internet of Things. It allows you to transfer data from one device to another without human interaction. For this, cellular communication is used, therefore mobile operators offer their services in the field of M2M.

The technology is used to transfer data from ATMs and vending machines, to monitor the condition of patients, in alarm systems and video surveillance. in fuel sensors. electricity and water meters, for tracking transport and cargo. Fog computing will allow machines to communicate faster and more efficiently.

Edge computing.

Edge computing is a technology for processing and storing data on the end device. They are even closer to the user than "cloud" and "fog".

Advantages:

• Virtually zero delay in data transmission. Calculations are carried out on end devices, so information does not need to cross kilometers of networks to reach the data center.

• Reliability of calculations. Data is processed even in the absence of an Internet connection.

• Security. All information remains on the device. It is not necessary to transfer it to the public cloud.

Disadvantages:

• Equipment and staff costs. The user of the technology will have to buy and configure the equipment, involve specialists. This is more complicated than connecting to a public cloud.

The fields of application of edge and foggy technologies overlap in many respects. Their main advantage is the speed of data transmission and analysis. Therefore, these technologies are used where real-time information processing is important - for example, in the fields of IoT and VR/AR.

In production, edge computing is needed for timely maintenance of equipment, in the oil industry, they will help detect malfunctions and leaks, and in the banking sector, the technology will allow you to quickly make a decision on a loan or detect fraud. In all examples, edge computing helps to operate without delay.

Edge is widely used in industrial enterprises. "Smart" equipment at enterprises does not always require a connection to the cloud to perform calculations - then network designers bet on the periphery and thus increase the efficiency of data processing.

Cloud development prospects.

Cloud technologies are rapidly being introduced into our lives. Retail and wholesale trade enterprises, production and the financial sector became the most active buyers of services.

Public clouds turned out to be the most popular of all - their costs accounted for 85% of costs. The rest was spent on private clouds.

Development of edge / fog computing

Companies are already starting to use edge and fog computing alongside clouds. Of course, these technologies are more developed in Europe - they are used by both large corporations and startups.

Large companies that sell cloud services are expanding their range. Microsoft offers not only the cloud, but also solutions with cutting edge technologies. For example, a system that allows you to transfer part of the calculations to IoT devices, or a border server for data processing with artificial intelligence. Amazon is also not far behind and offers its service for the Internet of Things with edge computing. At the same time, companies do not forget about the main product - data is not only processed on the periphery, but also transferred to the cloud.

New technological services help in processing data in production, where delays are a serious obstacle to work.

While government organizations are experimenting with connectivity, startups are implementing practical solutions. SONM works with fog computing - offers a platform with blockchain technology. The idea is to create a decentralized supercomputer. Users can rent out their computer power and join a distributed network. Companies, in turn, buy the capabilities of the fog platform for their computing.

Facemetric startup is also connected with granite technologies. It provides customers with video surveillance cameras and data centers with neural networks to search for images in video - faces, car numbers, price tags and much more. But storing and processing a large video stream in the cloud is difficult and not always advisable. Therefore, the company decided to use edge computing.

Trends in the development of cloud technologies.

Thus, cloud computing can be considered as a new approach that will give a powerful impetus to the further development of information technologies and computer sciences. Note that distributed and parallel computing in Europe and America has been widely supported. For example, over 1 billion euros have been invested in distributed and parallel computing in Europe over the past 10 years. Currently, the VENUS-Sp project is being developed in Europe, which is funded to reveal in more detail the possibilities of using cloud computing for research and industry.

Numerous and widely known technologies such as resource computing, grid computing, and virtualization are considered the predecessors of cloud computing. Hypervisor and much more. Service-Oriented Architecture (SO A) also played an important role in the development of cloud computing. Cloud computing is in some sense an extension of SOA applications. Recently, SOA, along with Web 2.0, has been more closely associated with "Mashup" technologies. From a technical point of view, "mashup" is a web application that combines data obtained from several sources into one integrated tool. Well-known examples of "mashup" are web services that use cartographic data from Google Maps.

The primary goal of enterprises and providers that embrace cloud solutions is to provide enterprise IT infrastructure as a service. Today, they try to apply the experience gained in the integration and provision of corporate applications as separate services in the organization of infrastructure levels. Software and physical infrastructure, like applications in SOA, are expected to be discoverable, manageable, and adjustable. There is a need to create specific standards that would describe how to discover, consume, administer and regulate services. Open standards are key to getting the most power and flexibility from using cloud technologies. And although the development of new standards is still ongoing, some of the new technologies are at the stage of active implementation. For example, for interaction with cloud services, there is now a standard that requires the use of client-side browsers that support AJAX technology. their offline operation must conform to the open HTML5 specification.

The cloud standard also does not limit the choice of software solutions that can be used for work. The modern set of solutions is called LAMP (acronym for Linux, Apache HTTP Server, MySQL and Perl / PHP / Python); data exchange is based on XML and JSON technologies (a textual data exchange format based on JavaScript), REST (REpresentational State Transfer) is expected to work with web services. This technology describes an approach where a fairly narrow set of standard formats should be used to work with data. Thus, the variety of methods of interaction between objects is strictly limited and the complexity of the involved protocols is reduced.

Standards that ensure the operation of application programs are important: support for functions based on HTTP and XMPP (Extensible Messaging and Presence Protocol, an open communication protocol for software of the Middleware class, based on XML), security tools (OAuth, OpenlD, SSL / TLS) and aggregation when transferring data (Atom).

For development teams, in addition to a ready-made runtime environment, the cloud provides another advantage': it can offer such a variety of SaaS as tools as a service. As a result, integrated development environment (IDE - Integrated Development Environment) and simple code editors become hosted programs available to every developer at any time. This eliminates the need for local development environments and. respectively, in licenses for each machine, which is convenient.

There is another factor in the impact of cloud computing on developers. In order to facilitate the understanding and maintenance of the source code, to simplify the interaction between developers when creating the same software, standard application programming interfaces (APIs) are created. Of course, developers strive to adhere to standards, but in some cases, non-standard APIs provide a certain performance benefit. In the cloud, however, any deviations from standard ARIs are particularly dangerous. Consumers know that they are receiving services from a cloud provider, but may not know the details of the implementation of those services. Thus, the advantage of cloud technologies is the universality of the solution.

Thus, it is possible to distinguish four directions that must be developed to ensure the security of cloud data center construction:

- secure data storage in cloud storage;

- safe execution of tasks;

- secure data transfer;

- secure data access.

However, as you can see, cloud technologies have more advantages than disadvantages. In addition, one cannot ignore the current trends in the development of the IT industry, in which the need to turn to cloud computing is increasingly visible, despite the lag of information protection systems.

The creation of new standards, including for ensuring the security of cloud technologies, is currently a priority task, and the further development of cloud solutions will be carried out together with the emergence of new, more reliable methods of data protection.

Some challenges and risks.

In the construction of large data centers, one can see the aspirations of some multinational corporations such as Microsoft. IBM, Google to master large volumes of information. The development of today's events can be presented as follows.

For example, a company reports that it has developed a cloud version in addition to regular software. In fact, the average user may not need the cloud version, but some company may use it. Although the convenience of collective use and the security of data storage are advertised, the data becomes available to the owners of the clouds, that is, to the owners of the servers.

The company can say that in the future it will support only the cloud version of the programs. Of course, you can maintain the usual version on your computer, but after a while the PC will fail, as initially, during production, a limited resource of its use time is laid. On the new computer, the "iron" will be changed in such a way that the usual version of the programs (not cloud) will no longer work there, as well as many programs from other companies. Thus, you will have no choice but to "go to the cloud", that is, your data will become available to outsiders.

Cloud file systems.

A cloud file system (distributed file system for cloud) is a file system with a distributed architecture that provides users with simultaneous full network access to data / files.

Goal:

- optimization of batch data processing (e.g., using MapReduce);

- high availability access to data in case of failure of system nodes;

- support for complex system topology (geographically separated nodes and clusters);

- support for larger files (up to several TB) and a large number of files;

- use of TCP/IP and extracted procedure calls for data access.

Characteristics of cloud FS:

- dividing files into blocks (a few MB) to optimize access;

- duplication of blocks on several nodes for fault tolerance. Geographically separated nodes are often selected to optimize access speed;

- dedicated servers for storing metadata (correspondence of blocks to files, position of files in directories).

Examples of cloud FS:

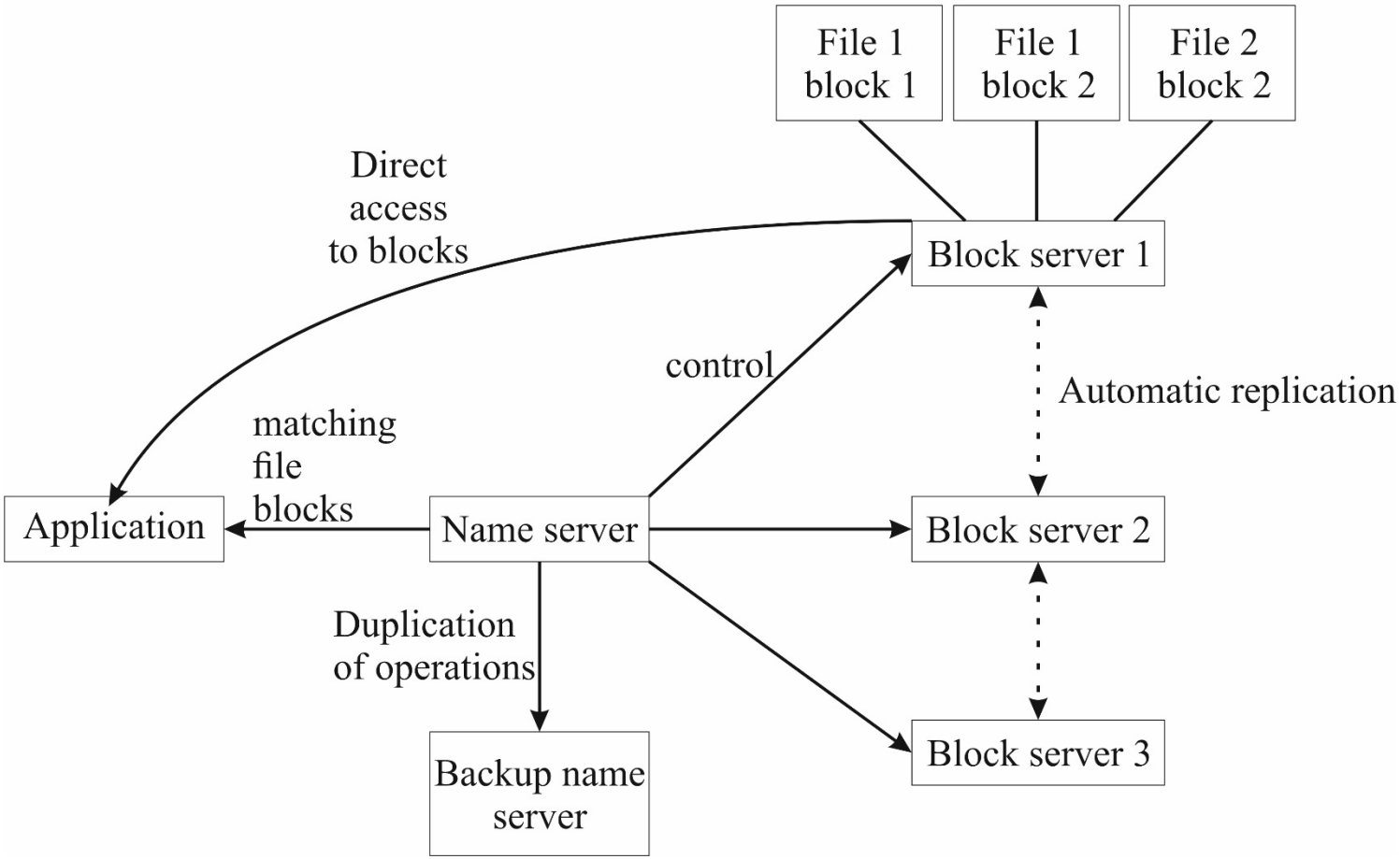
- Google File System;

- Hacloop Distributed File System (HDFS);

- Luster;

- IBM General Parallel File System (GPFS).

A typical architecture of cloud file systems



Web 2.0 technologies.

Web 2.0 technologies made it possible to run web applications directly in a web browser window, rather than running them on a local computer or on a local network.

Web technologies have become widespread in the field of education. Web technologies are information technologies, the use of which makes it possible to process web resources located in the web space of computer networks (local or global).

Web-space should be understood as an informational component of local or global networks, with the help of which web-resources (text, graphics, sound, video resources) are used. which are connected to each other by hypertext links.

the concept of Web 1.0 is considered as "read-only Internet". This technology allows you to search and read data and information on the network. It provides few ways for interaction with users and their participation in filling the Internet with new resources.

Web 2.0 is a method of designing systems that, by accounting for network interactions, become better the more people use them. An important feature of Web 2.0 is the principle of involving users in filling and repeatedly using content.

It is not for nothing that Web 2.0 technologies are called social network services. The term "social service" comes from the word "sociium" - community (a collection of people who have something in common, the basis of which is communication between people). This technology provides, first of all, network interactivity.

Here are some characteristics of Web 2.0:

-Users can change web pages. A good example of this is product reviews from users.

-Social networks. The age of social networking began more than a decade ago with Friendster and MySpace. The apogee has been reached today. With the rise in popularity of Facebook, Twitter and other social networks, web pages connect one user to another:

- Ability to instantly share information. Modernity needs speed in everything. "Hot" news is in demand. This is why Twitter and YouTube have become so popular. These services deliver information as quickly as possible.

-New methods of information gathering. Now an Internet user just needs to subscribe to the RSS feed (Really Simple Syndication) and receive news and updates.

-Access to the network from mobile devices. Tablet computers and smartphones now have access to the web, allowing more people to quickly find the information they need.

However, there are certain disadvantages of using Web 2.0 technologies:

- dependence on the presence of a connection to the Internet (connection disappears

- information becomes unavailable or inconvenient to use);

- the dependence of the quality of the service on the quality of the work of many other companies (the work of providers, companies to which the services belong, etc.);

- vulnerability of confidential data, saved on server pages (known cases of theft of personal data of users, mass hacking of blog accounts, etc.);

- violation of the law "On copyright";

- virtual dependence of a person.

The term Web 3.0 is interpreted as high-quality content and services created by professionals based on the Web 2.0 technological platform. His explanation for the emergence of Web 3.0 is that since Web 2.0 is a technological platform that allows you to create a number of services on its basis, many monotonous resources have appeared, which, accordingly, devalues the value of most of them. Therefore, the Web 2.0 technological platform is to be replaced by a third - cultural version of the Web, which will allow reviewing and selecting interesting and useful content.

The main idea of Web 3.0 is that the user, who previously participated in the content creation process alone, has the opportunity to create with the involvement of a team, in particular partners who are experts in the necessary areas of professional activity. The user status can be changed to expert, as well as the form of cooperation between the content developer and the portal. The expert acts as a moderator of the content published on the network. Web 3.0 foresees the emergence of highly specialized resources, where the aggregation of all the services and tools of the professional social component necessary for the user will be carried out and the publication will be carried out.

You can compare Web 1.0, Web 2.0 and Web 3.0 by various criteria. The following are the following:

- Participants;

- Software:

- The approach to content organization;

- Basic events;

- Value and cost.

It should be noted that with the advent of new Web technologies, the previous ones do not become outdated and unsuitable. The educational process uses both Web 1.0 technologies (for example, to work users with electronic libraries in online reading mode) and Web 2.0 technology. which allow:

- create websites (for example, with Google Sites);

- to keep a calendar, a work schedule, to make curricula, etc. (for example, with Google Calendar);

- create documents of different formats and edit them in conjunction with other participants in the educational process (for example, with the help of Google Document);

- use e -mail with spam protection (for example, with Google Mail (Gmail);

- create 3D models (for example, using SketchUp);

- keep diaries of educational projects (for example, with the help of Blogger);

- create photo albums, edit photos, work with graphic file editing programs compatible with other participants in the learning process (for example, using Picasa);

- analyze visits to sites, blogs, etc. (for example, with Google Analytics).

Problem Management of Resources in Service Systems.

The paradigm of cloud computing-the merger into a single information and computing space of arbitrary heterogeneous and about the part-time-shaped computing units in various administrative domains, with its local security policy.

We distinguish features of resource management, depending on the selected models of use. The Iaa and Paa models suggest that the dynamic characteristics of the applications are accidental, since the user can solve arbitrary tasks about the way it happens in general -purpose operating systems. The Saa model is different from the Iaa and Paa models in that the supplier controls the entire application cycle and can know in advance static and dynamic requirements for resources.

The task of management of resources is also complicated by the requirements for the quality of the service: the time of guaranteed response, the level of bandwidth, accessibility, failure, time of recovery after failure, etc. Therefore, there is no universal solution to the optimal management of resources in the Iaa and Paa models. Basically, research is conducted in the field of virtualization of elements of computing systems.

The SAA model provides more resource management opportunities. Knowing the characteristics of the task can be more accurately determined when and what resources should be obtained, taking into account the current state of resources of the distributed computing system (processor, RAM, device of introduction/conclusion and data transmission device).

Compared to SOA (service-oriented architecture- SOA), cloud calculations set more global task - to provide the service of calculations of any level not only at the level of applications, but also at the level of operating systems, specialized computing resources, etc. Cloud calculations introduce additional (non -functional) requirements for the service. Cloud computing systems should have elasticity, that is, the ability to use new physical resources while increasing and releasing resources while decreasing the number of custom requests. The concept of cloud computing covers issues related to reliability, adaptability, level of quality of service and many others, which are related to the construction and operation of real -life systems, compared to SOA. She only describes the scheme of construction of applications from the components.

Information security in cloud computing: problems and perspectives.

Standardization of cloud computing.

Since the technologies of cloud computing are just beginning their way to mass use, one of the main problems of ensuring security is the lack of generally accepted standards for the provision of cloud services. Consequently, there are no universally accepted standards in matters of cloud computing security. The problem of standardization in ensuring information security is in the process of being solved in three main directions.

The specifics of ensuring information security in cloud computing.

Let's consider the main advantages of cloud computing from the point of view of ensuring information security.

Cost reduction.

With the growth of the scale of computing systems, any measures to ensure security are cheaper on a per-user basis. The concentration of resources makes it possible to reduce both the initial and current costs of information protection (for example, the purchase of hardware protection tools, the use of enhanced authentication, backup copies, the involvement of information security specialists, the development and maintenance of the concept of information protection, the design and stabilization of production processes and etc.).

Optimizing the investment structure.

Cloud computing makes it possible to optimize two key indicators of the economic efficiency of the information infrastructure. Return of investments in infrastructure (return of investments, ROI) is easily planned and starts from the moment of using cloud services. The initial investment is reduced, consumers pay only for the resources, services and functions that are actually needed and ordered. Additional and unplanned investments on the part of the consumer are excluded, because in the event of service failures. the supplier is responsible.

The total cost of ownership (TCO) is in many cases lower than when organizing your own data centers. Costs for content, maintenance, risk mitigation, servicing and scaling. service personnel and associated costs (electricity, production space, insurance, fire protection) are included in the subscription fee.

Small and medium-sized enterprises can get the greatest effect from the optimization of the investment structure. Companies for which the operation of GHG infrastructure is not related to the main line of activity can avoid investments in non-core assets.

Improving data security and shifting responsibility.

The provision of cloud computing services implies high-reliability data storage and backup, fast recovery functions in case of failure, certified encryption of data during storage and during transmission between the provider and users. If all the listed conditions are met by the data storage provider in the cloud, it can be compared to renting a bank safe. The responsibility for ensuring information security at the appropriate levels is transferred from the consumer to the supplier.

When providing system resources from a supplier to a consumer in the form of a service, a number of organizational risks arise that must be taken into account when using cloud computing.

Let's consider the main types of risks Service provider dependency.

The lack of generally accepted standards can make the consumer dependent on the service provider. A necessary condition for minimizing this risk is the development, verification and support of the concept of data and application migration to an alternative provider.

Impossibility of compliance with newly emerging requirements.

The development of the service consumer's business may give rise to new requirements for the computing system that cannot be met when working with the existing supplier. To minimize this risk, the consumer needs to develop and implement production processes for monitoring, evaluating and planning the implementation of new properties and functions of computing processes in advance (release management).

Limitation of control over the services used.

Using cloud computing services, the consumer has not only limited responsibility for information security, but also limited control over the operated services. The degree of restrictions is determined by the chosen cloud infrastructure model and the provisions of the contract between the suppliers and the consumer.

The concentration and sharing of computing resources also creates a number of technical risks specific to cloud computing. Consider these risks.

Violation of data isolation.

Due to the collective use of system resources, cloud computing requires reliable isolation of user data from each other. The consumer should pay attention to the levels of the generalized data processing model at which other users participate in the computing process - at the infrastructure level (for example, virtual servers, shared hardware resources, etc.), at the platform level (for example, the used virtualization system etc.), at the application level (for example, database management systems, web applications and services, etc.).

The greatest danger in this regard is represented by systems in which a single hardware module (for example, a central processor), a piece of basic software code (for example, a virtualization platform), or an instance of an application (a process) will be used by several different users from different consumers in parallel.

Exploitation of cloud computing system vulnerabilities.

The data transmitted and stored in the cloud computing system can be compromised or falsified to circumvent the rules and processes of ensuring security as a result of the exploitation of possible vulnerabilities at various levels of the cloud computing system. Information about such vulnerabilities may become publicly available before the problem is resolved by the vendor.

To minimize this risk, it is necessary to use encryption of transmitted and stored data. At the same time, the organization of management of encryption keys and certificates used for data encryption in the organization - consumers of cloud computing services - deserves special attention.

Resource exhaustion and denial of service.

Exceeding the level of requests to services above the maximum permissible load, including due to DoS attacks (Denial of Service), can lead to the unavailability of the cloud computing system for users. In this connection, special attention should be paid to the guaranteed parameters of availability of computer systems and restoration in case of failures, which are provided by the contract between the supplier and the consumer.

Development incompatibility.

Hardware or software content issues (for example, platform-specific development with a platform API) can lead to security failures. To minimize such risks, it is worth paying attention to the certification of the hardware and software part of computing systems and services provided by the supplier, familiarizing yourself with the organization of support during operation (maintenance, restoration, etc.), choosing a model of computing infrastructure organization that provides for minimum requirements to the competence of users.

Conclusion.

The use of cloud computing causes not only significant economic benefits, such as reducing costs, optimizing the structure of investments, increasing data security and transferring the responsibility for ensuring security to the service provider, but also significant risks from the point of view of ensuring information security.

Considered types of cloud computing services and the main risks arising from their use, among which organizational (such as dependence on the service provider, impossibility of meeting new requirements, limitation of control over the used services) and technical (such as violation of data isolation, exploitation of vulnerabilities) can be distinguished cloud computing systems, resource depletion and denial of service, incompatibility of used developments), are the basis of recommendations for the transition to cloud technologies.

A fundamental and multifaceted risk analysis for information security is an integral prerequisite for the development and support of successful and effective information protection measures in the conditions of cloud computing.

Despite all the advantages of cloud computing, today consumers need to take a balanced approach to their implementation, organically combine traditional (local) and cloud infrastructures in the organization of the computing process.