

# **Obstacles on the way of successful adaptation of cloud services in Russia**

Dmitrii Piskarev



<b>Author(s)</b> Dmitrii Piskarev	
<b>Degree programme</b> BITe	
<b>Report/thesis title</b> Obstacles on the way of successful adaptation of cloud services in Russia	<b>Number of pages and appendix pages</b>
<p>In this thesis I will take a look at principles of cloud computing, and what obstacles there are on the way of its further adoption in Russia. I believe that cloud computing is a very current topic, and it is even more of a case in Russian business environment. Russian cloud market is currently falling behind European and United States' markets, although it is developing quite rapidly. Also, Russian market is quite unique in many ways, and I am expecting that it will have certain specific tendencies. I think that it is important to understand specifics of the Russian business environment and its specific obstacles on the way of the cloud in order to be able to predict the future trends.</p> <p>In order to understand the phenomenon better the report contains theoretical research on cloud computing, including its key characteristics, service and deployment models, and current trends. Then it will present qualitative research in the form of interviews with Russian businessmen in order to understand the specifics of the Russian market to the greater extend. All of the research was performed between October 2014 and May 2015.</p> <p>This thesis will cover the basics of cloud computing, its history and evolution, current trends, and what obstacles there are on the way of successful adaptation of cloud computing in Russia. It is intended mainly for businessmen, so the technical details are out of the scope. Also, the research is focused mainly on Russian cloud market, and therefore all the interviews were conducted with Russian businessmen only.</p>	
<b>Keywords</b> Coud services, Russia, adaptation of cloud computing.	

## Table of contents

1	Introduction .....	1
1.1	Justification of the topic .....	2
2	The research question and objectives .....	2
2.1	The research questions .....	2
2.2	The research objectives and the scope .....	2
2.3	Definition of the research .....	3
3	Cloud computing .....	3
3.1	Definition of cloud computing .....	3
3.2	Key characteristics of cloud computing by NIST definition .....	3
3.2.1	On-demand self-service .....	3
3.2.2	Broad network access .....	4
3.2.3	Resource pooling .....	4
3.2.4	Rapid elasticity .....	4
3.2.5	Measured service .....	4
3.3	Service models .....	4
3.3.1	Infrastructure as a service (IaaS) .....	4
3.3.2	Platform as a service .....	5
3.3.3	Software as a service .....	5
3.4	Deployment models .....	5
3.4.1	Public cloud .....	5
3.4.2	Private cloud .....	5
3.4.3	Hybrid cloud .....	5
3.4.4	Community cloud .....	6
4	History and the evolution of cloud computing .....	6
4.1	The dawn of virtualization .....	6
4.2	Technologies that paved the way for cloud .....	7
5	Specifics of transition to cloud computing .....	7
5.1	Economies of scale .....	8
5.2	Transfer of capital expenses to the operating .....	8
5.3	The cost of migrating to the cloud .....	9
6	Obstacles on the way of the cloud .....	9
6.1	World-wide legal issues with the cloud .....	9
6.2	Legal issue related to cloud in Russia .....	9
6.2.1	Processing of personal data .....	10
6.2.2	Cross-border transfer of personal data .....	11
6.3	Internet availability .....	11
6.4	Psychological conservatism .....	13

6.5	Security .....	13
6.5.1	Data breaches .....	14
6.5.2	Data loss .....	14
6.5.3	Account Hijacking.....	14
6.5.4	Insecure APIs .....	14
6.5.5	Denial of service.....	15
6.5.6	Malicious insider.....	15
6.5.7	Abuse of cloud services .....	15
6.5.8	Insufficient due diligence .....	15
6.5.9	Shared technology issue .....	16
7	Interviews .....	16
7.1	Marketing director of Compulink.....	16
7.2	Head of IT department of VTB bank.....	20
7.3	Manager of IT department of Gazprombank. ....	22
8	Conclusions and discussions .....	27

# 1 Introduction

In latter years, cloud computing becomes more and more popular for both private users, as well as companies of all sizes. And we can see that the number of people and businesses using cloud computing grows very fast. According to the data available on the Internet (Statista 2015), the popular cloud storage Dropbox had been adding about 100 million users per year in the last few years. In November 2012, they had 100 million users, 200 million users in November 2013, and by November 2014 the total number of users went over 300 million users. If we take a look at some of the more business-specific products, e.g. cloud-based project management software; we will see that they also have hundreds of thousand customers, with millions of users. It is difficult to give the exact figure for the total value of the cloud market, although it exceeds 100 billion per year, and it is going to grow further. According to Gartner (STAMFORD, Conn., February 28, 2013), “from 2013 through 2016, \$677 billion will be spent on cloud services worldwide”, and those are not the numbers to be ignored.

The Russian cloud market is not that big, even in comparison with such a small country like Finland. Nevertheless, the Russian market is also growing very fast, and the fact that Russia is behind means that there can be more opportunities. According to J'son & Partners Consulting (East-West Digital News, October 21, 2013), “by 2017 the market will reach not less than eight billion rubles (approximately \$250 million)”.

We can see that cloud is becoming more and more popular for both small and large businesses, and there are good reasons for that.

First of all, with the growth of the market a lot of new opportunities arise. There are much more options now than before, that cover most of the aspects of nearly any business.

There are cloud storages, project management software, customer relation management systems, accounting software, cloud platforms for software development etc. And all of those useful services do not usually come alone, but there are always options that would suit your particular needs. And even if there is no suitable application for your very specific tasks, it could be possible to design an application from the scratch to tailor it exactly for your needs.

One of the biggest advantages of cloud services is scalability. Because of the fact that you can easily scale your services towards current needs businesses can react much faster to the constantly changing environment, whether the impact is positive or negative. Another bonus is that scalability negates high initial costs. Licensing costs are reduced, because you are only renting the service rather than buying a right to own your own copy. This really helps smaller businesses, because high initial costs can be extremely significant downside to adopting new services. On top of that it is much more common for cloud ser-

vice providers to take care about all the updates, and include the price in the rent fee, which takes quite a lot of pressure from the users, who often does not have sufficient technical support to manage their hardware and software efficiently.

## **1.1 Justification of the topic**

One of the biggest problems that Russia is facing now is the fact that its government structures, as well as most businesses, are terrifyingly inefficient. The fact that Russia is behind the most developed countries in their use of cloud technologies is not only the effect of this situation, but also to the certain extent the cause of it. We can witness now that more and more companies as well as the government structures are trying to digitalize their business processes. Being able to understand what obstacles and hidden stones there are on the path of adopting cloud services can be very useful for those businesses that try to move forward and become more competitive and efficient, as well as for those, who see this rapidly growing market as a source of opportunities. And even more importantly, this information should help to move around those obstacles, and provide clues for where the market might be heading in the future.

## **2 The research question and objectives**

All of the questions of this research are targeted at people doing business in Russia, and the answers should reflect their own perspective.

### **2.1 The research questions**

1. What is cloud computing? What are its key characteristics, how did it evolve over time, and how is it applied in practice.
2. What are the main obstacles on the way of cloud computing? How the situation in Russia differs from the situation in other parts of the world?
3. How do Russian businessmen and experts see the current situation regarding cloud computing in Russia? Which obstacles or opportunities do they see?
4. What conclusions can be drawn from this information? What are the trends, and where will they lead us?

### **2.2 The research objectives and the scope**

The main aim of this research is to understand what Russian businessmen see as the major obstacles on the way of adopting cloud computing in Russia. In order to build a foundation for this, basics of cloud computing will be researched, as well as its history and the process of evolution of the concept, which will help to understand how it got to the current state.

The scope of this research only covers the business side of the problem, and does not look into technical details behind it. Its results should be useful for anyone with the minimal knowledge of computers. Also the research focuses mainly on the Russian market, and therefore interviews will be conducted only with Russian businessmen. Nevertheless, the theory part will be universal, and relevant not only in Russia.

### **2.3 Definition of the research**

The first part of the research will be the theoretical background, which will provide information on definitions of the concept of cloud computing, service models, deployment models, etc. Then I will look at the history and evolution of cloud computing, as well as the most common trends. After that I will take a look at the aspects of the practical application of the cloud computing, including some examples of the Russian software-as-a-service solutions.

In the second part I will take a look at the obstacles on the way of the cloud revolution. It will include problems that are typical for the cloud computing, as well as the comparison to the situation in Russia.

In the third part I will conduct my own qualitative research of the Russian businesses in order to learn more details about what is the current situation, and how do they approach cloud services, and the problems that they face.

## **3 Cloud computing**

### **3.1 Definition of cloud computing**

Cloud computing is an information technology concept that implies providing universal and convenient remote access to the pool of configurable computing resources, which can be promptly provided and released with minimal operating costs and on demand. Since its first appearance in 2006 the concept had deeply infiltrated different information technology fields.

### **3.2 Key characteristics of cloud computing by NIST definition**

There is a widely used framework suggested by National Institute of Standards and Technology (NIST), which incorporates the key attributes of cloud technologies.

#### **3.2.1 On-demand self-service**

The consumer has the opportunity to access the computing resources provided unilaterally, if necessary, automatically, without the need to interact with the staff of each service provider (Peter Mell & Timothy Grance, 2011).

### **3.2.2 Broad network access**

Computational resources available on the network through a standard mechanism for a variety of platforms, thin and thick clients (mobile phones, tablets, laptops, workstations, etc.) (Peter Mell & Timothy Grance, 2011).

### **3.2.3 Resource pooling**

Computing resources from a single provider serve multiple consumers on models of multiple rent (multi-tenant). Pools include various physical and virtual resources that can be dynamically assigned and reassigned according to the consumer demand. There is no need to understand or control on the part of the consumer the exact location of resources, but it is possible to specify the location at a higher level of abstraction (eg, country, region or data center). Examples of such resources can be storage, computer processing power, memory, network bandwidth (Peter Mell & Timothy Grance, 2011).

### **3.2.4 Rapid elasticity**

The resources can be flexibly allocated and freed (returned to the supplier) as soon as possible, in some cases automatically, to quickly scale commensurate with demand. For the consumer the possibility to provide resources may seem as unlimited, they can be assigned to any number at any time (Peter Mell & Timothy Grance, 2011).

### **3.2.5 Measured service**

Cloud systems and services should have the functions of automatic measurement, control and optimize the use of resources at the level of abstraction, with regard to all sorts of services (for example, the volume of storage, processing, bandwidth, or active user sessions). Use resources can be tracked and monitored, providing transparency for both the provider and the consumer using the service (Peter Mell & Timothy Grance, 2011).

## **3.3 Service models**

### **3.3.1 Infrastructure as a service (IaaS)**

The possibility of consumers handling systems, storage, data networks and other fundamental computing resources where the consumer can deploy and run arbitrary software, including the operating system and applications. The user thus does not control the underlying infrastructure clouds, but has control over operating systems, storage systems and deployed applications, and possibly limited control over the choice of network components (for example, a host with firewalls) (Peter Mell & Timothy Grance, 2011).



### **3.3.2 Platform as a service**

The possibility of the consumer to be deployed to the cloud consumer, created or acquired applications created using programming languages and libraries, facilities and services, supported by the service provider. The consumer, in this case does not control the basic cloud infrastructure including network, servers, operating systems and data storage, but has control over the deployed applications and possibly some configuration options hosting environment (Peter Mell & Timothy Grance, 2011).

### **3.3.3 Software as a service**

The possibility of the consumer to use application operating in the cloud. Applications are available from a variety of client devices, or through a thin client interface such as a web browser (eg, web mail), or the program interface. The user thus does not control the underlying infrastructure cloud, including networks, servers, operating systems, storage, or even individual application settings, except for some custom application configuration settings (Peter Mell & Timothy Grance, 2011).

## **3.4 Deployment models**

### **3.4.1 Public cloud**

Cloud infrastructure prepared for public use by the general public. It may be in the ownership, management and maintenance of the business, academic and government organizations, or any combination thereof. Cloud exists on the territory of the cloud provider (Peter Mell & Timothy Grance, 2011).

### **3.4.2 Private cloud**

Cloud infrastructure prepared for the exclusive use of a single organization consisting of several users (eg business unit or a part of a single holding company). This cloud can be in the ownership, management and maintenance of the organization, third party, or any combination of these, and is both within the organization and outside it (Peter Mell & Timothy Grance, 2011).

### **3.4.3 Hybrid cloud**

The cloud infrastructure that is a composition of two or more different infrastructures clouds (private, community, or public) that are unique objects, but are linked together by standardized or proprietary technology, allows you to transfer data between applications or components (for example, for load-balancing between clouds) (Peter Mell & Timothy Grance, 2011).

#### **3.4.4 Community cloud**

Cloud infrastructure is prepared for the exclusive use of a specific user community from organizations sharing common problems (eg, mission, security requirements, policy, and general requirements). The cloud may be in the ownership, management and maintenance of one or more organizations in the community, to a third party, or a combination of these, and is both within organizations and beyond (Peter Mell & Timothy Grance, 2011).

### **4 History and the evolution of cloud computing**

Despite the fact that cloud computing is based on relatively old technologies, its use was somewhat limited until 10-5 years ago. At the moment we are in the final stages of development of cloud technologies, still open for inventions, or adjustments in business models. The term cloud computing became wide spread around 2007, although it has much longer history. Most of technologies that come into the cloud paradigm had existed long before, although the market did not have the solution that would include them in a commercially attractive. During the past 10 years public cloud services that were both easily available for developers and clear for businesses emerged.

#### **4.1 The dawn of virtualization**

One of the key technologies that lay in the foundation of cloud computing is virtualization, which is nearly 50 years old. Virtualization was first suggested for IBM mainframes in mid 60s, although after the transition of computer technologies from expensive mainframes to much smaller and affordable personal computers based on x86 architecture virtualization was forgotten for quite a while. At that time virtualization was still a possibility only for those, who could afford mainframes.

It was not until mid 2000s when the situation begun to change rapidly. Until then the x86 VMware mostly monopolized virtualization market, although in time its monopoly was threatened by both commercial and open-source projects. Under their influence VMware made the desktop version of the software for launching virtual machines free. In 2006 Microsoft also made a free version of MS Virtual PC.

The first company that fully understood the commercial potential of widely available virtualization technologies was Amazon. Until 2006 virtualization was seen as an opportunity to run required number of virtual servers on your own hardware. Amazon Elastic Compute Cloud introduced the idea of running virtual servers on rented hardware, which is essentially the Infrastructure As A Service model. The benefits of such rent is obvious – all you have to do is pay for the service, and you immediately get a fully virtual server, which is just as good as your own server.

## **4.2 Technologies that paved the way for cloud**

Virtualization is very important, although it is not the only technology that laid the foundation for cloud paradigm. Among the other trends that worked as a prelude for the modern cloud computing were Service-Oriented Architecture (SOA), Application Service Provider (ASP), Information Technology Infrastructure Library (ITIL), IT Service Management (ITSM) etc. Some of those concepts included quite specific technological approaches, while others were mostly used as a marketing term.

Availability of widespread high-speed Internet connections made possible data exchange between computers in the cloud. Maturity of Web 2.0 allowed interactions with functionally rich applications right in the web browser, without the need to download them and launch on a local computer or in the local network. Internet services that allow access to their resources via special Application Programming Interfaces (API) also contributed to the success of cloud computing. When a developer is providing a service for remote users based on the data from the remote source (such as Facebook) it is quite logical that data processing would also be done on remote platform.

Cloud computing accumulated a lot of ideas from preceding concepts, and that is why it is a very versatile term. It is a technical paradigm, as well as a marketing term. Essentially cloud computing absorbed IT industry ideas from the couple of past decades.

## **5 Specifics of transition to cloud computing**

In the context of global excitement it is sometimes difficult to objectively judge the extent of usefulness of cloud computing. In real life economical advantages for one side can in some cases become disadvantages for another, and not always can adaptation of cloud technologies overcome the risks that it brings. So it is important to look what actual benefits does cloud computing brings. In this part I will use the understanding of cloud computing suggested by University of California at Berkeley In their understanding cloud computing is a collection of Software as a Service and utility computing. According to this model utility computing includes both Infrastructure as a Service and Platform as a Service.

SaaS is oriented on the end users, while both end users and other suppliers of SaaS service can demand utility computing. Therefore, it is possible for one participant in the cloud market to be both the supplier and the provider (Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia, 2009). The model does not take into account the private clouds, because they are too individual, and it is difficult to assess them alongside the private clouds. It is not the only approach to classifying the cloud

computing, although it is easier to assess the economical value of clouds using this model.

## **5.1 Economies of scale**

When talking about the economical benefits of cloud computing the most common economical effects relate to the economies of scale. Owners of large data centers are able to achieve competitive advantages over smaller datacenters because of the scale of their platforms. Unlike their smaller competitors owners of large data centers are able to significantly reduce the costs for electricity, network infrastructure and personnel.

Another reason why larger platforms are able to become more economically effective is because they are much less vulnerable to the uneven load caused by daily, yearly or industry related fluctuations. While private highly specialized platforms are built to meet the peak loads, larger data centers can afford to spread the load between users whose cycles of the resource use are negatively correlated.

Because of those reasons larger suppliers are able to save up to 30% on the hardware alone when comparing to smaller competitors. Very high entry threshold (building a large data center can cost hundreds of millions) means that perfect competition is highly unlikely in this field, at least in the near future.

## **5.2 Transfer of capital expenses to the operating**

Another very common argument is a possibility of replacement of capital expenses with operating (CAPEX/OPEX). If economies of scale relates mostly to the owners of data centers, that possibility of getting rid of capital expenditures sound very attractive for users of computing powers provided by those data centers – users of IaaS and PaaS solutions.

Transition of capital expenditures to the operational expenditures allows the company to avoid diversion of capital investments into non-core assets. With the current pace of IT advancement the amortization period for a server is about 2-3 years. Transition to cloud computing allows the company to free up the resources from investments into the hardware, and using those resources for something more useful.

Adopting cloud computing also allows the company to reduce the risks related to the exploitation of servers. If a company would decide to close an IT project, or the load would decrease because of the optimized software, the company would not be left with the excessive hardware, and will be able to easily decrease the amount of resources used. It is especially useful for pilot implementation, where the amount of required resources is the least predictable, and the perspective a project is not obvious.

### **5.3 The cost of migrating to the cloud**

It is easier to talk about the economical advantages of moving to cloud when the system is being created from scratch, because you do not have to consider optimizing and rewriting existing applications, compatibility with inherited systems, reeducation of employees, utilizing old hardware etc. Nevertheless, this situation is very rare, and migration to the cloud involves not only the economical benefits, but also the additional costs.

When developing new applications from scratch traditional model is much less attractive, because it involves a lot of additional one-time investments not only into development of application, but also in the hardware. In the long run it involves significant expenditures related to the use of own computing powers. But in the case of updating the existing system the cost of adaptation might make transition to the cloud much less attractive, or even not feasible.

## **6 Obstacles on the way of the cloud**

### **6.1 World-wide legal issues with the cloud**

Cloud computing is very inconvenient from the legal point of view. Internet became a platform for distributed applications: a company can keep confidential information inside an SaaS application that also uses resources or hardware of the other IaaS or PaaS provider, and all of them can be located in different parts of the world. Legal issues that arise from situations like that are difficult to solve using current legislations. What are each subjects right and responsibilities, how do they differ from each other, how do they differ in jurisdictions of different countries, how do those legislations interact with each other, etc.? All of those problems are still mostly unsolved, especially if we look at the global picture. Another problem of regulating the relationships in cloud computing is that interests of users and providers are very different. Users are interested in maximizing their data protection, while providers are interested in maximizing the freedom in terms of development of their services. This problem is quite typical for most new technologies, and will be solved eventually. Nevertheless, it still remains a problem for now.

### **6.2 Legal issue related to cloud in Russia**

The problems of cloud technologies are personal data protection are relatively new for Russia. In current legislation there are no obstacles for processing data in the cloud, and responsibility for use and protection of personal data can be passed on to the third parties, although it is quite difficult to apply current laws in many situations. Some providers argue that if the system would fit the requirements for the on-site version, then there is nothing preventing it from being deployed in the cloud. Although in some cases it is not possible to

build the system according to the legislations, and therefore it is not possible to create a solution in the public cloud, so there is only the private cloud option. The complexity of the situation is very individual and varies from one solution to another to the great extent because information systems are divided to categories depending on the types of data that they hold. In order to avoid problems with legislation, businesses have to perform an audit of all of their information, and optimize it accordingly. It is crucial to build at least the threat model, and implement the means for protecting local systems that process the personal data. This task involves a lot of work that requires a lot of finances, which is a lot more than most of the cloud service providers would pay in other countries. This is not a problem of the cloud as such, but rather of the chaos in the corporate IT legislations.

In the situation of excessive regulations there is always the risk that some of the suppliers would not comply with the requirements of regulators. Especially it is important in relation to the ФСБ (Federal Security Service), because according to the current requirements it is only possible to transfer data through the channels with the use specialized encryptions, which most of the smaller companies cannot afford. In some cases it is simply not possible to satisfy the current legislations, even if you try. It is physically impossible for some of the companies to satisfy all of the requirements of current legislations regarding the clients rights, personal information processing etc.

#### **6.2.1 Processing of personal data**

It is important to understand what processing of personal information in the cloud means. There is an opinion that provider of the cloud service is treated as a legal representative of the operator, and therefore in order to process data in the cloud platform he is required to have permission from the subjects of the personal data. The law states that it is required for providers (who are the third parties in this case) to have permission from the subject of the data. Although, if the provider obtains information from a third party, then he is required to inform the subject about the data being processed. Unless the subject refuses processing, the provider is allowed to use the data. Therefore, in order to process any personal data in the public cloud provider is required to obtain a specific permission. Also, it is required for operators to provide data regarding all its cloud providers, and list all the possible action that can be done with the data in the cloud platform.

Despite the fact that this opinion is based on the current legislation, in real life the situation is different. Most of the businesses tend not to comply with the law, but base their decisions on their own understanding of risks related to not complying the law. This is caused by the fact that within current legislation regulators requirements are too strict. Following the law to the letter, even if it would be possible, would mean that the business will lose its competitive advantage, or even would not be able to operate at all. Knowing this, businesses in Russia tend to keep their business process that involve processing of per-

sonal information as they see fit, until they are faced with an actual case of discontent from users, or trouble from the government.

### **6.2.2 Cross-border transfer of personal data**

At the moment cross-border transfer of personal data is not so much of an issue. Currently there are no restrictions on providing the personal data to any European countries.

There are certain restrictions regarding acquiring of permissions from subjects of the data in case of providing the data to third parties, although it is not a big issue.

Processing the data abroad can be quite beneficial for Russian cloud users. In this case they do not have to comply with Russian government structures legislations, and instead have to work with legislations of foreign countries, which tend to be much more adequate. On top of that European conventions restrict additional requirements and restrictions while performing cross-country data transfers, unless it is a matter of national security, and therefore there is no need for additional encryption of data.

The new version of the law regarding protection of the personal data will come in force on the 1<sup>st</sup> of September 2016. This law states, "when collecting personal data [...] the operator is required to provide a record, systematization, accumulation, storage, updating, retrieval of personal data of citizens of the Russian Federation, databases located on the territory of the Russian Federation" (Dan Worth, 2014). This is a major change that effectively means that IT companies providing services to Russian citizens will have to either move their servers to Russia, or seize their operations in Russia. Big companies have already taken actions to anticipate the change: Microsoft is planning to build additional data centers in Russia, SAP and IBM are negotiating renting computing and storage powers from Russian providers, etc. more companies mentioned that they are not planning to leave Russian markets, and will watch the changes of legislations closely. It is not possible to fully understand the implications of the law until additional related regulations will be in place. There are a lot of possible threats and opportunities for both foreign and domestic stakeholders. One of the important factors is that it might be very difficult to track data is used by applications, especially in the case of applications with the closed code. Russian businesses tend to easily avoid the excessively strict legislations, which might happen in the case of this new law. For example, a company would keep some data on Russian servers just for the show, but will actually use the data from the outside source.

### **6.3 Internet availability**

Availability of fast and affordable Internet channels is the key to successful adaptation of cloud computing. Even the simplest SaaS systems adopted in a company significantly increase the load on the Internet channel. Most of the major applications in the cloud-

computing field are created with American or European markets in mind. It is safe to assume that the quality of Internet connections in states and Europe are good enough for modern cloud computing, although some might argue that in Russia the situation is not as clear.

The level of prices for the broadband Internet connection in Russia are generally lower than in Europe or United States, although lower prices does not necessary mean that broadband Internet is cheap in Russian. If we would recalculate those prices in relation to the average GNP per person, we would see that the actual cost is the same, or even higher.

The average download speed of the broadband Internet connection in Russia got a lot better in Russia in recent years, and, according to <http://www.netindex.com>, is marginally slower than Europe and USA. An important factor that should be taken into account is that both prices and speed of the broadband Internet connections in different parts of Russia differs very significantly, and average results might not be as representative. European part of Russia, including two major cities (Moscow and Saint-Petersburg) will have much better download speeds for much less than cities in Siberia or in the Far East. Most of the major and most progressive businesses are accumulated around those major cities, and it seems that there are no major problems with broadband Internet there. Although if we will take a look at other parts of Russia availability of good enough Internet connection will likely to be an issue.

Another important factor that is specific for Russia is the difference between private and corporate tariffs for broadband Internet access. Prices for corporate customers are generally higher than for private users all over the world, simply because they tend to need more services and of higher quality. Although most of the times those prices are maximum twice as high, while in Russia corporate tariffs cost significantly higher. This means that for some smaller companies having a better Internet connection is a significant increase of costs.

Reliability is also an important factor. Adopting cloud technologies means that the requirements for the quality of services and reliability of the Internet provider increase drastically. A company that has its data in cloud storage, or whose business processes depend on availability of certain cloud application, simply cannot afford losing Internet access, because it can bring the whole operation to a halt. USA based providers seem to found a solution for this problem. In their practice it is common to openly publish detailed liabilities for the quality of services that come into the Service Level Agreements. In this case they are superior not only to Russian, but even to some European colleagues. In this scenario if a provider fails to meet the requirements, he is financially liable for the fault. The amount of payments to a single user is relatively small, although considering the amount of users the payments can be huge, which forces providers to ensure the level of



quality. Service Level Agreements include parameters like availability, latency, lost IP-packets, and even reactions to DoS attacks. Despite ridiculous prices for corporate customers in Russia, there is nothing of that sort.

#### **6.4 Psychological conservatism**

One of the difficulties of adaptation of any kind new technologies is psychological conservatism. Most of the people and companies are very resistant to change, and cloud computing can be a good example of that kind of change. The biggest problem is the lack of understanding of the subject, its pros and cons, and possible consequences of adaptation of new technologies. Especially it is the case for Russian government structures, but not limited to them, because in many cases they still have some kind of Soviet mentality, and strongly resist any kind of innovations. The reason for that is that innovations are mostly welcomed by generation of younger professionals, while in the government, as well as in many companies, key positions are still held by older people.

Another problem with cloud technologies, and automation in general, is that there is a question of what to do with the people who used to perform duties that are now being done automatically. This situation is worsen by the fact that nepotism is very common in Russia, in government structures as well as in big companies, which leads to sustained level of inefficiency and resistance to optimizations.

Adaptation of cloud computing in big companies and government structures also might case changes in financial currents within their structures, which can also be opposed despite of the obvious benefits. Reduced costs, as well as very low initial costs can also be undermined by the fact that companies had already invested significant amounts of money in there systems, and no one wants to admit that there is a better alternative.

#### **6.5 Security**

One of the most common problems of adaptation of cloud technologies is security. Cloud does have certain security risks associated with it, and it is important to understand them in order to avoid problems. According to the survey, the most relevant threats according to users are:

1. Data loss/Data leakage
2. Insecure APIs
3. Malicious insiders
4. Account/Service & Traffic Hijacking
5. Abuse of Cloud Computing
6. Unknown Profile Risk
7. Shared Technology Vulnerabilities

## 8. Distributed Denial Of Service Attacks (CSA, 2012)

### **6.5.1 Data breaches**

Sensitive information falling into the wrong hands is a threat, which existed long before the cloud computing, but with digitalization of the majority of business data it became even more of an issue, and more active use of cloud computing made the situation even worse. In case of a successful attack on the cloud server it is possible that bad guys would get access to all of your sensitive data, and possibly your clients' data as well, which can lead to devastating results. It is possible to protect yourself against those situation, and mitigate significant amount of risk, although it is not possible to eliminate all the risk, and as long as you use the cloud, there is always a possibility that some of the information will leak.

### **6.5.2 Data loss**

Depending on the situation, losing your data might be even more devastating than data leakage. Losing year's worth of work, or losing data that cannot be restored at all can be fatal for businesses. And if data breach in vast majority of situations is likely to be initiated by some kind of ill wisher, data loss can be caused simply by natural events. Apart from being someone's fault (e.g. provider's carelessness), it can be caused by unpredictable catastrophic events, or even your own mistake. Of course it is very important to store your data safely, create regular back-ups etc., although sometimes you just have to rely on your provider of the cloud service, and nothing in this world is perfect.

### **6.5.3 Account Hijacking**

Account hijacking is one of the threats that is mostly dangerous for the cloud services, because by definition you have to use the web and some sort of account authentication. Such methods as phishing, fraud, and exploitation of software vulnerabilities can lead to results varying from relatively harmless to complete loss of control over your data. The big problem of this particular type of threat is that most of the times the weakest link is the user itself. If for any reason you fail to notice that you are on the phishing website and enter all of your authentication details there, then you practically gave bad guys all they need to get full access to your account, and password strength, encryption methods etc. do not matter anymore.

### **6.5.4 Insecure APIs**

Some cloud providers allow the use of APIs for their services, and as it is with most of enhancements, those additions can increase the risks. It is very important for the user of a

cloud service to understand the possible implications of the use of such software interfaces, and ensure that they are designed properly, and are protected against malicious attempts accordingly.

#### **6.5.5 Denial of service**

Denial of service is seemingly less dangerous threat, but it is compensated by the fact that it is much easier to perform. In the case of distributed denial-of-service attack, it is quite ironical that scalability of cloud computing power is what makes it easier to perform. Denial-of-service attacks do not damage your data, or give access to the inappropriate users, although it prevents you from accessing it. Nevertheless, considering the timing and other factors, it is possible to significantly damage a business simply by not denying access to a specific data.

#### **6.5.6 Malicious insider**

According to CERN (<https://www.cert.org/insider-threat/>), an insider threat is “A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.”

The problem with this is again that a particular person is a weak link here. It is possible that this insider would be a member of your team, or an employee of the provider. Since in most cases you are not able to affect the provider's staff, you really don't have much control over it, and therefore is constantly exposed to this risk.

#### **6.5.7 Abuse of cloud services**

Scalability of cloud services can be turned to bad cause, and easily available computing powers can be used for DDoS attacks, cracking encryption etc. This threat is more viable for cloud providers than for customers, and we won't look too much into it.

#### **6.5.8 Insufficient due diligence**

The biggest threat to businesses that come from cloud services is the lack of understanding of risks and implications. Most of the threats can be countered, or at least mitigated, although that would only be the case if the appropriate measures would be taken. Lack of basic knowledge of the subject will leave all of the data stored in the cloud and beyond extremely vulnerable to attacks, as well as accidents.

### **6.5.9 Shared technology issue**

With all of the delivery models, the case with the cloud services is that a provider provides a similar service to many clients. This means that in this multi-user environment there is a risk of shared vulnerabilities, which would leave the whole provider's cloud of users compromised.

## **7 Interviews**

### **7.1 Marketing director of Compulink.**

#### **How would you assess the level of readiness of Russian businesses for transition to cloud computing?**

I would begin, perhaps, with the definition of cloud computing. In addition to the three service models - IaaS, PaaS and SaaS, - there are three deployment models: private cloud, public cloud, and the hosted cloud. Public clouds are the clouds of global Providers: Microsoft, Google, Amazon, and so on. They have their own datacenters with which they use to provide cloud services, including on Russian territory. Currently no global providers have datacenters in Russia, although it is about to change, especially in the light of the new legislation. Hosted clouds are the clouds of service providers, which are typically located near their consumers, like Parking.ru, Infobox, Oversan, Masterhost, etc. Private clouds belong to the specific organization.

If we are talking about private clouds, there are no significant problems: in general, organizations are ready to use them. We can see this in the current practice: there is a lot of projects, both pilot and industrial, to introduce private "clouds". The only obstacle to the implementation of private clouds is the need for standardization of IT services, which are used in the organization. After the company manages to standardize its own services for internal users it is ready to use the private cloud.

#### **Can you give examples of standardized services that Russian companies can adopt in their own private "clouds" at this stage?**

Take a look at the implementations in Svyaznoj. One of the tasks that were possible to solve here is the fast provision of infrastructure for testing. Previously it took IT department about two days to provide the necessary hardware infrastructure for testing new applications. With the help of the private cloud they are able to perform the same tasks within hours. This is the example of the standardized service – the provision of virtual servers. The characteristics of those servers are also standardized: we can determine the typical configuration for them to deploy them faster.

**So, the service in this case, is it a server with certain characteristics, or the application that operates on the remote server?**

It is certainly both. Any IT service in the company that can be virtualized can also be standardized. The company should catalogue its standard services that it is supplying to itself.

**Can we say that in the future all of today's data centers will be in the cloud?**

Private clouds have so many advantages and so technologically attractive in terms of management that everyone will come to that eventually. The question is which applications it will affect. It does not always make sense to move the entire load to the cloud. Sometimes it is better to leave some on the pure hardware, or even keep it outside of the company.

It also linked to the technological maturity. If we take UK as an example, then we will see that 40% of infrastructure in large and mid-sized companies is outsourced. It is unclear when Russia will rise to the same level.

**What should companies that already invested in their own infrastructure do?**

Yes, indeed, there are companies that invested a lot of finances in their own data centers. The biggest companies in terms of management are multi-branch networks, which are served by several data centers. Although those companies do not have the task of minimizing costs, there are different priorities. In this case private cloud is implemented to provide more adequate infrastructure for business. Therefore we are talking about scalability of applications, faster deployment of infrastructure for new applications and projects, including deployment of virtual machines, interactive monitoring, configuration management etc. – those technological advantages are very important. So we are not talking about some kind of extra investments, but about receiving more return from the existing infrastructure and more rational management of further development.

**It turns out that the initiative for the implementation of cloud computing in this case comes from IT, not from the business. Can the paradigm change at some point?**

I think that the key argument for business is the quality of their services, and if private, public or hosted cloud helps to improve the quality of service, then IT department should choose infrastructure that will be optimal for satisfying the service-level agreement. This is why we are saying that there will be no mass migration into the public clouds and refusal from private data centers. Cloud computing will reach the hybrid model, that will have elements of both models.

**Is Russian public sector ready for the cloud?**

In government structures the situation is significantly worse. The level of IT maturity is much lower, although it is a matter of time, and the lag is not critical. There are structures that work on the very high level, and they will be able to set the pace. Although, an important obstacle are the requirements for the deployment of information. In case of the current legislation talking about the full-scale use of cloud services by our government structures is premature. I think that the most perspective model is community cloud, when some kind of cloud provider that could provide services all around Russia will emerge.

**So the readiness of the public sector for adoption of cloud computing is depended on the provider?**

On two things, to be more precise. First is the quality of IT management in the public sector as a whole, readiness to standardize the infrastructure, and to optimize the IT systems. The second is availability proposals. Supply should satisfy the demand.

**According to your observations, how Russian approach to implementation of cloud technologies differs from the foreign?**

Lets start with which types of business differ the most. Of course, we are talking about the startups and online businesses. Look at how many such companies emerge in USA and Europe. New businesses and websites are being created on constant basis. Those super innovative young startups show good example to the rest of the industry, and the rest follow their lead. The situation in Russia is different, because we do not have such examples to follow, and it shapes the market accordingly. Availability of high quality broadband Internet and experience of users in Russia is lower than in USA and Europe.

**Apart from the innovative startups, what are the specifics of the approach to the cloud computing in Russian companies?**

If we are talking about the corporate customers, there is a tendency to build your own IT empires in Russia. It is a dream of every IT director to build his own data center. It is not the case in Europe, because there his aim is to satisfy the requirements of the business, and to keep his place. Building your own data center does not always help as, nor does it help to improve the quality of service. Here I would like to mention the lack of dynamics in the Russian market. If we will take a look at top 100 of the Russian market, we will see that in the last decade they did not change much, and with the top 10 the situation does not change at all. In USA the market is much more dynamic, and infrastructure has to respond to changes much quicker. In USA merges and acquisitions are much more common, and companies have to have infrastructure that adapts to the situation much faster. As soon as the Russian market will become as dynamic, infrastructure will soon follow.

On the other hand, Russian corporate sector might as well become the leader in terms of cloud usage. Big companies will build their own data centers and will switch technologies to the private clouds. It will eventually raise the question of investments in non-core activities. Why would financial or media institution have extremely expensive data center on its balance? After that data centers will either be moved into outsourcing, or will be sold or transferred to someone else.

#### **How can a problem of lack of qualified specialists be solved?**

First of all there should be a desire to learn, kind of a need, the feeling of inner discomfort from inconsistency of your knowledge according to your position. Secondly, as they said in Microsoft, 80% of learning happens during the work, and only 20% outside of it.

#### **How would you assess the dynamics of implementing of cloud computing by the segment – IaaS, PaaS, SaaS?**

I believe that the future lies in PaaS, and SaaS will become the niche for the complete applications based on PaaS. IaaS will, of course, still remain, although the future is mainly linked with PaaS. If we will take a look at the percentage of standard software used by companies we will see that there are replicated software, although there are also non-standard solutions personally created, or tailored for particular company. In Russia this number is much smaller, because there are not as much independent software vendors. In USA on the contrary standard software is used not as frequently. Most likely with time the percentage of non-standard software will rise, which will lead to growing demand of PaaS solutions, because it is the most efficient and the easiest way for deploying software.

#### **What other obstacles do you encounter while promoting cloud computing?**

I would say that the most common is the lack of practice. People don't tend to become pioneers in some kind of new technology, and our economical ecosystem does not stimulate interest in those innovations unfortunately. In USA if a company sees an opportunity to reduce costs by 1% and increase margin by 10% they would take the risk. If they would succeed is a different question, regardless of that the culture of innovation is much more common. We do not have as much pioneers who feel the need to get rid of its own infrastructure. Nevertheless, they begin to appear.

## **7.2 Head of IT department of VTB bank**

### **What is your opinion on cloud services?**

I observe the development of cloud technologies from two points of view. From one point of view I am the professional corporate IT specialist, and I am happy that information technologies are developing, and the industry will gain new ideas. From the other point of view I am a top manager of a bank who is interested in saving money, and I understand that cloud ideas will not introduce any radical changes to the bank, while still require significant financial expenses. And I am not alone in my conservatism. While talking to my colleagues from other banks and major companies I see that many of them are sure that cloud is just a marketing feature that is aimed at gaining additional financing from additional clients.

In my opinion there is nothing technologically revolutionary in clouds. Public cloud is kind of a new mental paradigm, which holds new threats and opportunities for all of us, and should be strictly regulated by law from the point of personal data protection and customer rights. Regulation of possibility of removing any kind of personal data from any resources on demand is a good step towards legitimizing public cloud infrastructure.

The private clouds from technical point of view are simply the common centralized applications that serve business interests. Renting software as a service is an interesting option for smaller companies that use standard applications. For newly established companies it is a very attractive possibility of an easy start, which help to reduce costs and time significantly. It is obvious that standard software will work just fine for small businesses, which are much less sensitive to data leakage.

There are no so many SaaS users in Russia, therefore the market has a very good potential. Nevertheless the question of responsibilities of suppliers remains open. In the case of SaaS a company moves the data outside of the perimeter of its internal network. If SaaS provider is a Russian company, then it involves some risks for their users, because this information falls out of control of its security service. If we are talking about the foreign companies, then this information becomes extraterrestrial. From one point of view it is much better protected from the Russian government structures, but on the other hand it is not clear how are they going to exercise its legal functions. It is not a secret that classical raid in an office generally starts with the seizure of computers and servers by the “competent authorities“. In the case of a foreign provider it is not possible to seize anything, or get the access to any information by legal means.

### **So, do you think that the government will oppose active promotion of clouds?**

No, I don't think so. Government will no mind clouds up until the point when there would be enough practical situations when corporate information would be unavailable to law



enforcement agencies. It is not a secret that some Russian companies seek to keep their sensitive data abroad. It would be possible that using SaaS based outside of Russian borders would become a massively popular. That is why the government is interested in regulating the rights for the deployment of information and personal data.

**Did VTB had any experience with cloud applications?**

Again, cloud applications for corporations are simply well integrated virtual applications that are deployed in a corporate network. All in all, it is not an innovation. We are using this kind of approach for quite a while now in our corporate information system. Cloud is just a new name for the existing paradigm. I would not object if one would interpret it as a transition to the cloud if the market dictates it, if it helps to better understand what do we do, and if it helps us to exist in some kind of trend.

Using SaaS is constrained for us by the lack of standard applications that would fit the requirements for functionality, agility and productivity, as well as by regulations regarding bank operations and protection of information.

Nevertheless, I will mention one single example of the use of an outside service. It is an application that helped us with recruiting. We use it because the hustle of caring about the rights of users for their personal data is their responsibility. When a new employee is recruited and provides his personal data to the bank is one thing, and a potential candidate posting his personal data on some kind of resource without signing any kind of written liabilities is a totally different thing. That is why we decided to use the service of an outside provider in order to pass the responsibility of keeping the personal data on them.

**How did you solve the problem of elasticity of resources for personal data centers? Did you purchase extra resources, or did you manage to achieve an internal elasticity by combining and optimizing the computing tasks?**

Like in many large companies virtualization of computing resources has reached quite a high level. We have not been buying any hardware for any specific tasks for a few years now. Every single application is given required part of resources – memory and processing power. It does not matter where the resources are physically located any more. It is a cloud in a way, because it happens in computing cloud. Nevertheless, it used to be called virtualization, and everyone was happy with that.

**Are there any non-critical systems that you are ready to deploy on a hybrid of public platforms?**

Well, maybe only the systems that are oriented for the outside functions. Even the banks portal is too critical for that, because we use it to provide remote services valuable information about our products. So, I would say that we are not prepared to deploy any signifi-

cant part of our resources on the outside platforms, and I do not think that this position is about to change any time soon. At least not before the legislation regarding bank secrets will change.

**What is your strategy for the future regarding clouds?**

Our cloud strategy is to integrate internal resources in order to build a kind of an internal cloud by uniting the existing systems. In this case the level of comfort for users will increase, because there would be no need to move the data from system to another. It will be as comfortable to use as cloud Internet applications.

Obviously there are significant problems associated with specifics of banking field, because integration of banking resources is much more difficult comparing to most of the other fields. Nevertheless, we are oriented towards comfort and usability of modern Internet resources, and would like to avoid cumbersome and outdated systems. In this sense cloud computing seems very useful.

**7.3 Manager of IT department of Gazprombank.**

**How do you assess the state of cloud computing in Russia?**

If we would compare the Russian market of cloud computing to those of USA or Europe, we will see that it is a bit underdeveloped. Not even in terms of technologies, but in terms of understanding of how to deploy information in public clouds. On top of that our legislation is kind of unpredictable, and the main obstacles lie not in technological or infrastructure factors, but in the legalization of clouds. The habit of using clouds would require a period of adaptation, which is mostly relates to human factor than to the technology.

**Which specific problems did you encounter with the current legislation?**

First of all I mean the notorious law about the protection of personal data. It is not just the law, but the maturity of the society for which this law is created, and which will comply it. From my point of view it is important not to run into extremes. We could try to close everything, and switch off all the computers. It will help to reach maximum security and perfect level of data protection. But this kind of protection will kill the business, and there should be more reasonable solution, which will allow both protecting the personal data and allowing business to prosper.

**Would it be possible to say that legal requirements prevented some kind of actual implementations in your company?**

I would not say that they prevented implementations, although they did slow many of them down. This federal law requires a serious attitude. When we talk about complying with its

provisions, including the questionable ones, there are a couple of approaches: there are those who take the risk, and those who choose more conservative position. I do understand the consequences of reckless decisions that were not thought through enough, although conservatism, complexity and lack of transparency of legislations led to many of our projects being significantly delayed because they were loaded with tasks that related to information security.

In general, it is necessary to look at the problem of compliance with the legislation comprehensively: it includes not only questions of information security and preparing the infrastructure, but also calculation of risks that the bank is willing to take. If we will stick to the most conservative approach, then we will have to essentially close the service of Internet banking, providing online profiles, etc., which will eventually lead to great losses and will make the bank uncompetitive. It will bring us back to the 90s in terms of level of service, which is not acceptable.

### **Is Russian financial sector ready for implementation of cloud computing?**

Despite cloud technologies being a part of our strategy, I am still relatively conservative, because I do not feel that this concept is mature enough. I think that maturation of cloud concepts in Russia requires few more years. But that only concerns public clouds, because creation of private clouds is possible even now.

### **How do you define private cloud? Is it just a virtualization of corporate infrastructure?**

Yes, although this virtualized infrastructure must be multi-user. Also it is crucial to have resource monitoring, virtualization management, automated resource allocation, possibility of dynamic scaling, as well as understanding of related costs. It is not possible to avoid financial part, because clouds involve significant investments, which should be compensated by optimization of working process.

### **There is an opinion that using cloud computing in banks is prevented not only by legislations, but also by simple lack of trust in outside providers, especially considering the fact that banking market is already saturated in Russia, and banks compete between each other for existing clients. Do you agree with that?**

Generally yes, I agree. Every bank is interested in keeping its financial data safe. But let's take a look at how banks evolved in USA. Their data is often processed in other countries, like India for example. Practically no one knows where the data is located, and it does not really bother anyone. Therefore we are back to the problem of market maturity, and the cultural behavior.

Lets take a look at the example of online trading. When we just begun to transfer the data via Internet, we were all very scared that it would be stolen. And, of course, from time to time it was, but just like it was stolen from physical banks as well. Therefore we are talking about the required adaptation period, which is likely to happen faster, because every new technology makes the adaptation for next one easier.

**Is there anything that can be done to speed up this process?**

Maybe we need a special voluntary certification of security of cloud solutions, similar to the certification of websites that will ensure the required level of privacy and data security. It has to be some kind of consortium that specifically deals with certifications for clouds. When a provider of a solution will be able to post a stamp, just like trusted Internet resources can post the eTrust stamps, then people would feel more confident when using those resources, and it will associate with a sign of serious approach.

**How willing is your bank to use SaaS solutions for non-key applications?**

We do use some of those applications: for example, we use it to receive the credit history and other information. But as for transactional applications, using SaaS is highly unlikely. Maybe in the case of analytical systems, or systems for market analysis, it might be possible, but providing the data from CRM system to some kind of cloud provider is hardly relevant. It would be much more interesting for smaller companies that are not interested in infrastructure related costs and application support. The situation is very different for big companies, and it is difficult to assess the possibility of relying on an outside provider in the case of CRM. Although I do not deny the possibility, because IT outsourcing was initially perceived with hostility, but everyone eventually got used to that. That is why the bank chose a strategy of slow turn towards new technologies, and we constantly keep new possibilities in sight.

**How actively do you experiment with new cloud technologies?**

We do have several pilot implementations related to desktop virtualization. In a sense it is the trial of new technology that had already proved to be efficient. While testing we work closely not only with IT block, but also with representatives from businesses in order to be able to see better how the technology works with the distributed platforms. Only after receiving evidence of positive results we will be able to come up with suggestions regarding new infrastructure.

**Have you encountered any kind of troubles during the course of pilot projects?**

Yes, we did. First of all it is the immaturity of technologies, but also the lack of competent resources, both internal and external. But it is the normal process of establishing of a new paradigm. It requires time and prepared infrastructure, processes, people and technolo-

gies. It requires to accumulate the critical mass and to make the initial capital investments, and only after some time the technology starts to work for us.

## **8 Deputy chairman of the Information Technology and telecommunications of the Vologda region government**

**How serious in your area is the problem of a lack of IT resources that can be compensated with the help of cloud computing?**

Indeed, in many regions, the problem of shortage of IT resources is very serious, and the Vologda region is not an exception. I would have broken the problem of a lack of IT resources, into two parts: on the one hand, the hardware, software and network infrastructure, and, on the other hand, the IT staff.

So, Vologda and Cherepovets - are the largest centers with a population of over 300 thousand residents. Cherepovets, moreover, is a major industrial center. For those cities the issue of infrastructure is not so relevant, and is solvable. But the question of shortage of specialists is sharp enough. On the one hand, there is a good training base in the form of universities and institutes that train specialists in the field of IT, on the other hand - the proximity of Moscow and St. Petersburg leads to an outflow of trained personnel from the region - this is due to various reasons, including lower wages.

But as for the rest of the, the problem of infrastructure and specialists is very serious, to the point that experts are absent. I mean, these professionals who can properly maintain the infrastructure, on the one hand, and those who can competently support and develop application software - on the other.

**Can we say that cloud computing will facilitate the task of regional informatization?**

The short answer is yes, of course. But you have to think about how it can be done. Take the infrastructural problems for example. Yes, indeed, the creation of the "right" data center and access to it can solve the infrastructure problem. But who will they belong to? I am convinced that it should belong to the regional subject. For profit companies use both their own data centers and data centers belonging to other large companies, such as "Megaphone". Why is the data center that serves the government and the municipalities should belong to the regional subject? There are many reasons, and it is difficult to explain all of them.

**Could you at least name the most important ones?**

For the most important reason I would mention the following. Firstly, security and access mode to restricted information. For example, information to the Department of Finance, for obvious reasons, can hardly be placed in the outside data center. As is the case with fi-

nancial information on the activities of the authorities. And it's not that officials want to hide something, but the fact that the leak of such data may be used for personal gain. And that does not include the fact that the government has state secrets, and the data for internal use only. Secondly, I am skeptical about the typical decisions at the regional level, and I believe that the management of software infrastructure, including the development, should be concentrated in the subject. Third, the use of joint data center will be hindered due to the huge amount of information that must be stored in the data center, for example, the level of federal district. Finally, the data center level entity may organize the work of even small municipalities that cannot afford to pay for services cloud large data centers.

**Do you think it possible to create a collective "cloud" for the needs of regions and municipalities?**

This question is difficult to answer. I just want to say that the subjects are very different from each, and something right for one might be unacceptable for another. This is associated with many problems - in particular, the fact that each entity has its own legislature, and its laws. By the way, this is not a problem for the federal government - it is possible and necessary to use standard solutions, the same for all the territorial bodies of the Federal government. As for municipalities, they also differ from each other not only in different regions but also in the territory of one territorial association.

To conclude, it is possible to say that it is possible to build a cloud in order to solve particular subjects typical problems. Although it is not possible to build one cloud for municipalities of different subjects.

The problem of cloud computing is largely a problem of standard solutions, and sample solutions, as you know, are not working in the municipalities at the moment. Every single one has its own specifics. It is possible to solve some problems of municipalities with the cloud. As for the number of data centers, each entity should decide for itself. For example, the Vologda region should have two data centers, according to the the number of large cities.

**Are there any significant obstacles to the use of third-party IT resources in the regional and municipal informatization?**

No, there are no specific technical problems. There are political as well as security and regime of access to information. Many municipal leaders are worried that their data would be located in a data center, and they are not able to provide the proper mode of using this data. It seems to me that this issue is primarily in the plane of legal regulation.

## 9 Conclusions and discussions

During this project I have made the research of the theory behind cloud computing, and the qualitative research of the opinion on the topic of Russian high profile businessmen. Researching theoretical background helped me to understand the concept of cloud computing to much greater extent, and allowed to provide the view on the concept for the reader. It did not involve technical details that would be difficult to understand for non-professional users, and therefore is mostly useful for those who are only vaguely familiar with the topic, such as businessmen, or non-IT specialists. It also involved some information about the history and evolution of the concept of cloud computing. The theory part also included the list of the general obstacles on the way of adaptation of cloud computing, as well as some that are specific to the Russian market.

The second part included interviews with high profile Russian businessmen, who are responsible for the IT aspect of the business. It was done in order to get a deeper understanding of problems that exist in the reality of Russian cloud computing market, and to be able to better understand their roots and implications. This gathered information led to several conclusions.

First of all, I was able to draw a conclusion that despite the fact that Russian market is behind USA and Europe, the situation has a strong tendency for improvement. Although problems such as Internet availability and conservatism are still an issue to the certain extent, their implications are diminishing. The potential of the Russian market is very high, and more and more people starting to see arising opportunities, while technological advancements help to utilize those opportunities. It has to be noted that the progress in European part of Russia is much faster than in the regions, although it is possible that advancements in the bigger cities (such as Moscow and Saint-Petersburg) will pave the way for the rest of the country by setting an example.

Secondly, the research helped me to realize that the biggest obstacle for adaptation of cloud computing in Russia is the problems with the current legislation. Most of the interviewed expressed their concerns about the problems that Russian laws regarding security and personal data processing create for businesses. Effectively, it is nearly impossible to follow those laws to the letter, and most businesses have to balance advantages of cloud computing with the risks that using them arise. It is difficult to say what exact implications the new laws will have, although they are very questionable. It seems that the reason for that is not only the immaturity of the market and lack of practical knowledge of the legislative powers, but also the specifics of Russian politics. It is quite possible that this kind of excessively harsh laws have a specific purpose. It is not a secret that the most power in Russia lies in the hands of law enforcement structures, and the fact that effectively every business have to bend the law to the certain extent gives them even more control. The

fact that now it is effectively illegal to keep the personal data outside of Russian borders makes the situation even tougher for many businesses. Nevertheless, at the same time it can raise a lot of opportunities for Russian market, because despite the fact that Russian data centers at the moment are hardly competitive comparing to the foreign alternatives, it is obvious that they will be developing in the upcoming years.

Because of those obstacles it can be concluded that currently the biggest potential for the bigger companies lies in private clouds, because it gives those companies the most control.

I consider the project successful, because its aims were met. Nevertheless, I think that one of the significant downsides of the research is that interviews were conducted with the people who are part of the large companies. That means that this research is biased towards the bigger companies, and miss out on problems that relate to smaller businesses.



## References

Statista 2015. URL: <http://www.statista.com/statistics/261820/number-of-registered-dropbox-users/> Accessed on: 28.05.15

Rob van der Meulen, Janessa Rivera 2013. Gartner Says Worldwide Public Cloud Services Market to Total \$131 Billion. URL: <http://www.gartner.com/newsroom/id/2352816> Accessed on: 28.05.15

East-West Digital News 2013. Report: Russian IaaS market to reach \$250 million by 2017. URL: <http://www.ewdn.com/2013/10/21/russian-iaas-market-to-reach-250-million-by-2017/> Accessed on: 28.05.15

Peter Mell, Timothy Grance 2011. The NIST Definition of Cloud Computing. URL: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> Accessed on: 28.05.15

Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia 2009. Above the Clouds: A Berkeley View of Cloud Computing. URL: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf> Accessed on: 28.05.15

Dan Worth 2014. Russia readies cloud laws to force Google, Microsoft to keep data in nation. URL: <http://www.v3.co.uk/v3-uk/news/2353556/russia-readies-cloud-laws-to-force-google-microsoft-to-keep-data-in-nation> Accessed on: 28.05.15

<http://www.netindex.com/> Accessed on: 28.05.15

CSA 2012. Top Threats to Cloud Computing Survey Results Update 2012. URL: [https://downloads.cloudsecurityalliance.org/initiatives/top\\_threats/Top\\_Threats\\_Cloud\\_Computing\\_Survey\\_2012.pdf](https://downloads.cloudsecurityalliance.org/initiatives/top_threats/Top_Threats_Cloud_Computing_Survey_2012.pdf) Accessed on: 28.05.15