

Troshina S. M., Lukyanenko S. D.

# ANALYSIS OF THE METHODS AND TECHNOLOGIES OF INFORMATION SECURITY IN CLOUD SERVER

*Low level of information protection when using the cloud server creates the threat of incidents. Terrorist and extremist organizations use the information vulnerability of cloud servers to create a risk of technogenic catastrophes. Species analysis of the characteristics of cloud technologies and existing remedies allowed to make suggestions for strengthening information security in this field.*

**Keywords:** cloud computing, server, encryption, filtering, authorization, identification, authentication, unauthorized access, transnational crime, organized crime, man-made disasters, information security.

## 1. Introduction

Competition in the provision of new information products is shifting from the market of goods and services in numerous sets of Web applications for working with documents. One of the forms of competitive struggle with segments Amazon S3, Crash-Plan providing online storage capacity of gigabytes, are cloud storage.

Cloud storage – a model of online storage where data is stored on multiple distributed network servers, giving consumers the information services, mainly third party. In contrast to traditional models of data storage on their own dedicated servers purchased or leased specifically for such purposes, quantitative characteristics, as well as the internal structure of servers is hidden from the consumer information services. Data is stored and processed in the «cloud» that represents the collection of servers that are located remotely from each other geographically, including continental.

The cloud is an online service that provides the ability to store files on a remote server. Download e-documents and their subsequent adjustment by the user is made to online storage on the server. It seems that all operations occur in one place, so-called «cloud». However, actually, the remote server is often located on different territories, and sometimes on different continents. The usability of cloud services de-

pends on the speed of the Internet connection established by the consumer, which should be 600 Kbps and above. Cloud services appeared in Russia together with high-speed Internet with a minimum speed of 1 MB/s.

## 2. Comparative analysis of cloud servers

Analysis of cloud storage services allows to reveal their advantages over traditional information systems, as well as significant information security weaknesses that may lead to the violation of personal data protection of users, as well as to man-made disasters of various scales.

Types of cloud storage services vary depending on their characteristics: compensated and uncompensated, are designed for a large amount of information and the small volume that creates support for various operating systems, etc. Species similarity of cloud servers lies in the way processing of information.

Service Dropbox supports Android, iOS, WindowsPhone 8 (partially). Service features: in Dropbox there is no document editing, no limitations on the format and size of media files. The service allows you to configure automatic syncing and uploading photos and video content to the cloud in real time, which guarantees the safety of recorded material in case of breakage information media.

For product promotion on the market of products offers several tariff plans with attractive economic conditions of the contract of purchase and sale: free 2 GB of disk space, which can be increased at the expense of attraction of referrals (new users who registered in Dropbox on the recommendation) and install the application on your computer. Privileges provided by the manufacturers of mobile devices. For example, during the registration process with some devices from Samsung and HTC additional amount of cloud storage Dropbox, and the right savings bonuses (53 GB for 2 years).

The Service Yandex. Disk: supports Android, iOS. To use Yandex. Disk you need to create an account that provides access to all Yandex services. This service allows you to link this entry to any of the accounts in social networks and implemented through not login, or login to the system directly.

For the promotion of Yandex. Disk used economic levers to attract customers. By default, users available 3 GB, after performing certain actions (e.g., installing an application on your computer, download the same file in the repository and posting the link to the service in social networks) increases the quota up to 10 GB, this number will increase to 10 GB is inviting referrals. In addition, the purchase of some laptop models is encouraged Samsung free provision of 250 GB.

The server only allows you to upload and download files, the files can be made public - in this case, they are not indexed by search engines, but are available via direct links, which you can send by mail or post in social network. Because of the proximity it has the largest speed (2-3 MB per second) and the ability to map a drive via WebDav. However, there is a drawback: there is no extension used the Internet.

Service GoogleDrive: Gmail users are getting «the load». The main advantages of the Google server is the low cost of an additional Gigabyte and tight integration with Google Docs allowing you to edit your files online, and then to Refine them locally in any office package. In comparison, the same online integration with Microsoft Office is endowed with the SkyDrive server.

The server MicrosoftSkyDrive: there is tight integration with Windows 8. A Live account used for working with Windows Store and sync settings in the operating

system, so SkyDrive will have to connect to the system automatically, and 25 GB is provided to the user free of charge.

The server is characterized by a high capacity RAM. Server SkyDrive on this feature below possibilities Yandex. Disk. The disadvantage of server Microsoft is that it does not support Linux or Windows XP.

The server is SugarSync's ability to sync any files and folders on the disk. In other services this function can be applied using hard links, however, as practice shows, it is not effective. The opportunity to limit the use of the communication channel, however, to limit in SugarSync only allowed to Upload.

Increase account made by a consumer through an invitation of a large number of users for a referral link. The only service that offers a similar referral system (Dropbox), limits the maximum bonus is 60 GB.

Some of the drawbacks of SugarSync servers is not high speed file downloads and no reference is made to a synchronized directory on the sidebar of dialogs for saving/opening files, which makes quick access to the right files.

Listed species characteristic of the cloud servers with the analysis of their advantages and disadvantages leads to the conclusion about the existing problem of information security in the cloud technology. Information security is one of the most actual problems of Informatization.

Cloud servers are created on infrastructural platforms with a high degree of automation. Cloud servers use traditional software and physical security: firewall, IDS/IPS, virtual closure of vulnerabilities (Virtual Patching) and antivirus programs. However, the problems arising in risk management.

### **3. Problems of information security in use of cloud servers**

The economic benefit of cloud technologies is obvious. However, the use of cloud computing increases the risk of emergence of emergency situations of technogenic character. The lack of physical access to servers in public cloud environments increase the need for improved security. When you have an emergency in the cloud server there is no possibility to press the emergency shut-off valve, in comparison with a physical server.

Transnational cloud-based technologies are widely used by organized crime in

accordance with the report of the international expert group of The Global Terrorism Index, information from the Global Terrorism Database (GTD), National Consortium for the Study of Terrorism and Responses to Terrorism (START). In Russia, the terrorism index is 6,76. Russia takes the 11th place out of 124 countries in terms of the threat of terrorist activity. Terrorist activities are closely linked to the receipt of illegal proceeds from trafficking in arms, drugs and slaves. Detection and investigation of crimes of terrorist and extremist nature with the use of information technology is complicated due to their cross-border and significant differences in national systems of criminal law and criminal process.

Crimes in the sphere of information security are qualified on set with the crimes against persons, law enforcement and economic crime [1].

Russia had recorded a total of 356 extremist crimes, in subsequent years their number increased: in 2008, 460 in 2009 to 548 in 2010 to 656 in 2011 to 622 in 2012 – 696, 2013 – 896, and in 2014 – 1024 crimes [2].

Conflict of laws Federal law of 25.06.2002 № 114-FZ «About counteraction of extremist activity» [3] and the Criminal Code of the Russian Federation, defining the conceptual framework and, consequently, of offences with similar symptoms [4], practically impedes the criminalization of extremist formulations. Also, extremism is part of propaganda and public demonstration of Nazi paraphernalia, which is in compliance with article 20.3 of the administrative code of the Russian Federation an administrative offence.

In the Supreme Court's determination presents a normative interpretation of the sign of extremism «humiliation of the dignity of the individual is the negative evaluation of personality in a generalized form, directed to her discredit, undermine the authority of the person in their own eyes» [5]

The legislation provides for the qualification for extremist activities – dissemination of information inciting hatred on racial or ethnic affiliation of individuals and peoples, using mass media, including the Internet. However, judicial practice, this provision is interpreted broadly, convictions, justified the use by criminals for extremist purposes any technical means, including sending SMS messages, which can create the effect of publicity. [6,7].

The threat to national security is that information systems and resources are used by cyber criminals to promote in the society the ideas of terrorism and extremism. The functioning of the cloud facilitates the Commission of crimes of an international character, due to the low level of protection of the reference data contained in cloud servers, and high conspiracy of malefactors.

Attackers use for the deepening of delinquency features cloud server: scalable; the payment of the product as; self-service; universal access; pooling of resources of large computing power; a need for constant connection; the possibility of breaches of confidentiality of stored information; low reliability; a security vulnerability. When penetrating the cloud server, the attacker has access to a huge data warehouse.

Conventional crimes in national law as crimes, committed by an organized criminal group [8]. Active promotion on the market of new information technologies requires a cloud of servers in combination with existing traditional methods of creation of new automated systems for registration of information dissemination of malicious content.

Extremist crimes with use of information technologies acquire a greater danger to society because organized criminal groups are involved a minor, as major users of transnational information systems [9]. Cloud servers are used more often by people aged under 16 years. Therefore, the organizers of criminal groups using the method of indirect Commission of crimes involving persons under the age of head of responsibility.

To combat international crimes [10] and overcoming harmful factors in information using cloud servers requires a systematic approach of legal, information and technical security measures with the use of automation.

In fact, to improve information security, on the one hand, apply proven tools and techniques: data encryption and remote key management. On the other hand, a prerequisite for increasing the level of automation is the integration of different security functions with a broker of cloud services. Consideration of these two aspects will allow you to take full advantage of the cloud and prevent information security incidents.

It is necessary that all servers on the local, internal or external clouds were identified and integrated into the concept of safety management. When using cloud services, the effect is achieved through direct integration with the broker of cloud services, which quickly provides information about the availability of different cloud servers. To map the parameters of the exploited servers, with the requirements of security systems in dynamic environments is not possible, because in the attempt of comparative analysis there are numerous errors.

The problem is that, if any cloud server is not integrated into the safety management system, the attacker he is elected for behaviour incidents. When information about all cloud servers is granted automatically, regardless of their location, using security profiles, you can actually make changes for any number of cloud servers.

#### **4. The Traditional means of information protection in cloud servers**

Automation simplifies tracking of changes made on the cloud servers, for example, in files or the registry. To reduce the complexity of tracking such events, it is necessary to provide automatic filtering of the reference data by specialized software. Need to automatically sort all the events, for example, when you upgrade standard system Linux or Windows. Thanks to the automatic filtering of «positive» events, you receive the opportunity to learn more about the remaining events. This allows you to detect potential unauthorized activity, identify vulnerabilities, and, on the basis of the analysis report on the incidents, to introduce additional measures of protection.

Providing secure cloud servers for data processing — is the primary preventive measures when using cloud services. The result of improvement of information security, hosted cloud server, that is outside of the realm of physical access.

As protection of information during transmission using cloud-based systems are used encryption methods. However, the duecord are transmitted in an unsecured form and without integrity. For secure record processing, it is mandatory to encrypt their transmission. Which will provide the user an increased level of security.

Increasing the level of information security is achieved by encrypting virtual hard disks. If necessary, obtain access to authorized users data is decrypted when

read, and then re-encrypted when written to disk. The result is protection from the unauthorized transfer of unencrypted information into long-term storage service providers in the form of backups.

When encrypting record there arises the problem of protecting the keys. Storage in the cloud is impractical because the accessibility to cloud servers or templates entail access to the key thus decrypted record. Set password at system startup, as is customary in on-premise solutions for record encryption, is difficult in the cloud server in the absence of this console. Physical enter key is replaced by the request that the cloud server sends to the external source to the key management server (Key Management Server, KMS).

The KMS server verifies the identification data, for example, cloud server, IP addresses, patterns or location. Also checked the integrity (firewall, installed patches, the presence of active virus scanner) a cloud server that sent the request. The process coincides with the traditional encryption of hard disks. If successful, the key is provided either automatically or after confirmation by an authorized person. As a result cloud server accesses record. The cancellation is the incident of violation of its integrity or identity.

Also encrypt hard drives with separate control keys perhaps the provision of Infrastructure as a Service, IaaS. Its use is advisable when implementing delivery models Platform as a Service, PaaS. So encrypted information in databases in clear text misses the provider's cloud servers. It is necessary for the work with the encrypted record keys are controlled by the user.

In server, Amazon S3 Server-Side Encryption the data is encrypted by the provider before moving it to storage or backup. This technology allows you to protect the information from attackers with physical access to hard drives (stolen data would be unusable).

However, these protections do not have effectiveness in the Commission of a crime by a person using his official position, as to the subject composition includes employees of the cloud service provider abusing his official powers (article 159.6, 274 of the criminal code R F).

An interesting variant of the encryption is a combination of encrypted data and secure transmission technologies.

The majority of SSL and VPN option support the use of digital certificates for authentication, by which before data is validated identification information of the other party. Such digital certificates can be stored on virtual hard disks in encrypted form. Their use is possible after validation by the key management server identity information and the integrity of the system. Consequently, the use of comprehensive measures of protection allows users a choice of cloud servers that were checked.

It is important to understand that the legal responsibility for the safety of the database and their loss is the responsibility of the users themselves cloud servers.

### **5. Conclusion**

1) To ensure information security in cloud servers, it is necessary to apply automated methods of screening incoming information. The method of automated filtration of messages will allow detecting the security incident, and to analyze vulnerabilities and to take preventive measures to strengthen the existing system of protection;

2) To implement an automatic encryption system for the transmission of information by the cloud server providers before enrolling its customers with increased protective procedures for transfer and use of keys.

3) To create special units of the Federal security service of Russia on the analysis and processing of information flows, stored and transferred in the cloud server and other databases, with the aim of combating extremism and other crimes committed with use of means of information.

4) To create an automated system for the registration of malicious messages and information stored in cloud servers and other databases, with the aim of preventing technogenic catastrophes.

### **6. Acknowledle**

Implementation of the proposals in the practical activities of the Federal Security Service of Russia and other law enforcement agencies will lead to decrease in risks of emergence of emergency situations of technogenic catastrophes.

---

## REFERENCES

1. Kochoy S. M. Terrorism and extremism: criminal-legal characteristic// Moscow: Prospect, 2005. P. 106.
2. The official website of the Ministry of internal Affairs of Russia. – [Electronic resource]. – Access mode: <http://www.mvdinform.ru>
3. Federal law of 25 July 2002 № 114-FZ «On countering extremist activities» // [Electronic resource]. – Access mode: <http://www.consultant.ru/online/base/?req=doc;base=LAW;n=76617>
4. The instruction of the Prosecutor General of the Russian Federation and the Ministry of internal Affairs of the Russian Federation dated October 28, 2010 No. 450/85/3 «About introduction in action of the Lists of articles of the Criminal code of the Russian Federation, used when forming the statistical reporting» // [Electronic resource]. – Access mode: <http://omamvd.ru/Data/Extrem/Docs/1/1.pdf>.
5. The definition of the Supreme Court of the Russian Federation dated 08.04.2010 No. 65-O10-1 // [Electronic resource]. – Access mode: [http://sudbiblioteka.ru/vs/text\\_big3/verhsud\\_big\\_44992.htm](http://sudbiblioteka.ru/vs/text_big3/verhsud_big_44992.htm)
6. The resolution of the Plenum of the Supreme Court of the Russian Federation of 28 June 2011 № 11 «On judicial practice on criminal cases about crimes of an extremist orientation» // [Electronic resource]. – Access mode: <http://www.rg.ru/2011/07/04/vs-dok.html>
7. The official website of the Prosecutor General of the Russian Federation // [Electronic resource]. – Access mode: <http://genprok.gov/ru/news/news-12016/>.
8. Resolution of the Plenum of the Supreme Court of the Russian Federation of 10.06.2010 No. 12 «On judicial practice of consideration of criminal cases about the organisation of criminal community (criminal organization) or participation in it (her)» // [Electronic resource]. – Access mode: <http://www.rg.ru/2010/06/17/prest-org-dok.html>
9. Chaika Y. Annual report of the Prosecutor General of the Russian Federation the Council of Federation of the Federal Assembly of the Russian Federation // Russian newspaper. Central release No. 5164 (85) dated 22 April 2010.
10. The Declaration on measures to eliminate international terrorism from 09.12.1994/ Electronic resource: // [http://www.un.org/ru/documents/decl\\_conv/declarations/terrdec1.shtml](http://www.un.org/ru/documents/decl_conv/declarations/terrdec1.shtml)

---

**TROSHINA Svetlana M.**, PhD, Associate Professor of chair «Theoretical Foundations of Radio Engineering» IRIT-RTF Ural Federal University First President of Russia  
B. N. Yeltsin  
E-mail: [troshina-svetlana63@mail.ru](mailto:troshina-svetlana63@mail.ru)

**LUKYANENKO Stanislav D.**, master of science of chair «Theoretical Foundations of Radio Engineering» IRIT-RTF Ural Federal University First President of Russia  
B. N. Yeltsin,  
E-mail: [mad-mike2332@yandex.ru](mailto:mad-mike2332@yandex.ru)

Трошина С. М., Лукьяненко С. Д.

# АНАЛИЗ МЕТОДОВ И ТЕХНОЛОГИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ СЕРВЕРАХ

*Низкий уровень защиты информации при использовании облачных серверов создает угрозу инцидентов. Террористические и экстремистские организации используют уязвимости информации на облачных серверах, что создает риск возникновения техногенных катастроф. Видовой анализа характеристик облачных технологий и имеющихся средств правовой защиты позволил внести предложения по укреплению информационной безопасности в этой области.*

**Ключевые слова:** *облачные вычисления, сервер, шифрования, фильтрация, авторизация идентификация, аутентификации, несанкционированного доступа, транснациональная преступность, организованная преступность, техногенные катастрофы, информационная безопасность.*

---

**ТРОШИНА Светлана Михайловна**, кандидат юридических наук, доцент кафедры «Теоретические основы радиотехники» ИРИТ-РТФ Уральского федерального университета имени первого Президента России Б.Н. Ельцина  
E-mail: troshina-svetlana63@mail.ru

**ЛУКЪЯНЕНКО Станислав Дмитриевич**, магистр кафедры «Теоретические основы радиотехники» ИРИТ-РТФ Уральского федерального университета имени первого Президента России Б.Н. Ельцина  
E-mail: mad-mike2332@yandex.ru