DOI: https://doi.org/10.36910/6775-2524-0560-2022-47-04
UDC 004[657+005]338.4
Zalialetdzinau Kanstantsin, software engineer Brimit LLC
https://orcid.org/0000000319380122

AUTOMATION OF ORGANIZATIONS USING CLOUD TECHNOLOGIES: SECURITY ISSUES

Zalialetdzinau K. Automation of organizations using cloud technologies: security issues. The article reveals the principles of automation of organizations using cloud technologies through the prism without the peak aspect. The main stages of development of cloud technologies are characterized, the advantages of using these systems in everyday work are revealed (low consumption of financial resources, possibility of universal access to information, constant improvement of software and technologies). At the same time, attention is drawn to the main challenges facing users of cloud services: the need for a constant and uninterrupted Internet, the inability to recover information in case of loss. Security remains a major issue, therefore. The purpose of the article is to analyze the risks and possible ways to overcome them in the work of organizations with cloud technologies. It is established that the system that affects the reliable storage of information from customers can be exposed to such threats as cross-site-scripting, fishing, Trojans, viruses. This is due to the fact that, as a rule, consumers working with the cloud computing service, use an Internet browser. In order to optimize information security at this level, you need to use licensed anti-virus software packages, personal firewall tools, tools to encrypt data or information on disk, a properly configured Internet browser. It is proved that the security of virtualization mechanisms also affects the reliability of the virtual environment. For example, if the attack is organized on the monitor of virtual machines, the attacker may unnoticed by the security system, which are in the virtual machines can edit, copy or block the flow of information. Thus, if a hacker gains access to control capabilities, he will not only be able to edit data, but also steal it throughout the virtual network. Therefore, to avoid this situation, you need to protect the administration or servers of virtual machines. In addition, you need to create specialized information security tools that can monitor traffic inside the required server. At the same time, compliance with basic fire safety rules is also important for the safe operation of servers.
Key words: cloud technologies, security, virus, information.

Золялетдінов К. Ю. Автоматизація організацій із використанням хмарних технологій: проблеми безпеки. У статті розкрито принципи автоматизації організацій із використанням хмарних технологій крізь призму безпекового аспекту. Охарактеризовані основні етапи розвитку хмарних технологій, виявлені переваги використання цих систем у повсякденній роботі (мала витрата фінансових ресурсів, можливість універсального доступу до отримання інформації, постійне удосконалення програмного забезпечення та технологій). Водночас, звернено увагу на головні виклики, що стоять перед користувачами хмарних сервісів: потреба у постійному й безперебійному Інтернеті, неможливість відновлення інформації у випадку її втрати. Вагомою проблемою, отже, лишається забезпечення безпеки. Мета статті – проаналізувати ризики та ймовірні шляхи їх подолання при роботі організацій із хмарними технологіями. Встановлено, що система, яка впливає на забезпечення надійного збереження інформації у клієнтів може піддатися таким загрозам як cross-site-scripting, phishing, трояни, віруси. Це пояснюється тим, що, як правило, споживачі працюючи із сервісом хмарних обчислень, застосовують Інтернет-браузер. Із ціллю оптимізації інформаційної безпеки на цьому рівні, потрібно на боці клієнта використовувати ліцензійні пакети антивірусних програм, засоби персонального брандмауера, засоби для шифрування даних чи інформації на диску, правильно налаштований Інтернет-браузер. Доведено, що безпека механізмів віртуалізації також впливає на забезпечення надійності віртуального середовища. Наприклад, якщо атака організована на монітор віртуальних машин, то зловмисник може непомітно для системи захисту, які знаходяться у віртуальних машинах може редагувати, копіювати чи блокувати інформаційних потік. Таким чином, якщо хакер отримає доступ до можливостей керування, то він зможе не просто редагувати дані, а й викрасти їх по всій віртуальній мережі. Тому для того аби уникнути цієї ситуації потрібно захистити до адміністрування чи серверів віртуальних машин. Крім цього, потрібно ще створити спеціалізовані засоби захисту інформації, які зможуть контролювати трафік усередині необхідного сервера. Водночас, дотримання елементарних правил протипожежної безпеки також важливе для безпечної роботи серверів.
Ключові слова: хмарні технології, безпека, вірус, інформація.

Introduction and problem statement. The use of cloud technology is very popular among Internet users because it contributes to ease of operation, and cost-effectiveness and generally improves the quality of user experience. This, in turn, contributes to the popularization of cloud technology in the IT services market.

The advantage of cloud service is the possibility to work with necessary information all the time having only a computer or a laptop. Moreover, cloud technologies allow you to adjust the corporate IT infrastructure quickly, taking into account immediate needs, and consuming exactly as many resources as necessary. Due to its popularity, the use of cloud technology is constantly improving, so their use in the work is constantly updated, and in the direction of improving and facilitating. The use of cloud technology, as follows. Allow to minimize the cost of digital operations, and avoid the purchase of expensive network equipment, complex hardware, and software solutions.

In general, cloud computing allows organizations to achieve some advantages in two fundamental categories of business and technology efficiency - faster time to market and increased agility. However, these approaches to evolving cloud technologies can create security gaps and human error. There are other potential drawbacks to cloud adoption in small businesses, including platform mismatch, network vulnerability, unreliable data, and business interruption. There may also be challenges in working with these technologies. For example, working with cloud technology requires staying online, that is, without an Internet connection to work with such services is not possible, this problem is still difficult to overcome, although recently developed mechanisms for an emergency, but slow communication, which will allow to obtain from the "clouds" only critical information needed in urgent cases. It is also impossible at this stage of its development to restore lost data, which may be very relevant in case of unpredictable circumstances. The latter is also possible due to the neglect of security rules, which is a vulnerable side of cloud technology users.

Cloud computing brings convenience and benefits to an organization, such as elasticity of business, lower costs, automatic hardware, and software updates, elasticity, and scalability. The main advantage is that it helps reduce unnecessary costs such as the purchase and maintenance of hardware and software. It also reduces the number of people working in IT. However, like all technologies, cloud computing has some problems. The biggest problem is security, especially data theft. More organizations will only want to use cloud computing if the problems are solved. Therefore, the security of the cloud computing service must be put first. Cloud service providers must ensure compliance with regulatory requirements that may be of concern to users. Through compliance, it helps users to be safety certified. In addition, security, policy should be provided by the details of access control, risk management, backup, and system recovery. Due to time constraints in the future, several examples will be chosen and discussed regarding how organizations have benefited from cloud computing. A theoretical framework will also be used to discuss how organizations use the framework. Different types of attacks always occur in the cloud environment, so a strong theoretical framework and architecture will be offered, especially for security. This is an important step needed for a cloud service provider to deal with a cyberattack.

Analysis of recent publications and research. The problem of using cloud technology is a hot topic for research, given the modern development of the computer system and the general Internet. Domestic science has not paid due attention to this topic, but foreign scientists have repeatedly drawn attention to the imperfect development of techniques for the security of digital information channels. In particular, Attaran M. and Woods J. characterized the problem of using cloud technology to improve enterprise operations [5]. They believe that cloud computing technology is a revolutionary way to harness the power of the Internet, providing software and infrastructure solutions to enterprises around the world. The authors mainly focused on the use of this technology in small businesses. Consequently, their work explores the specifics of using cloud technology in different types of small businesses, with Attaran M. and Woods J. referring to its successful practical application in Europe. In general, the system of cloud computing allows organizations to achieve some advantages in the two fundamental categories of business and technology efficiency - faster time to market and increased agility [5].

At the same time, Xu S. and Xin F. investigated the main advantages and challenges of cloud computing implementation in business. The researchers believe that nowadays the important task of modern organizations is to improve and automate the traditional ways of doing business. For this reason, they note that cloud computing is considered an innovative way to improve business. In particular, they play an important role in addressing inefficiencies and increasing business growth, helping organizations to remain competitive [10]. Creswell K. et al. outlined the major challenges and opportunities for cloud technology in healthcare. Their study is based on interviews with more than 20 individuals, mostly professionals working for large cloud providers, small and medium-sized software vendors, and academic institutions [6]. Skale M. also characterized the features of the implementation of automation processes in enterprises using cloud technology. He believes that security capabilities are the main obstacles to further adoption of cloud technologies because cloud systems are often a key target for cybercriminals [9]. For this reason, the protection of cloud platforms and information remains important. Ukrainian specialists have also investigated the problem of using these technologies. In particular, Litoshenko S. and others investigated the use of cloud computing to automate the accounting process but in accounting systems [2].

Kulik V. described the process of using cloud technologies in accounting and enterprise management. The researcher presented the key models of cloud computing aimed at the end-user: private,

public, public, and hybrid clouds [1]. At the same time, Liubimov V. and others highlighted the key problems of implementation strategy and increasing demand for cloud technologies in the IT market [3]. In addition, they believe that the pattern of cloud computing is due to the need for ubiquitous and comfortable network access. Consequently, this problem is quite widely represented in modern science.

Highlighting the previously unresolved parts of the overall problem. Therefore, the paper will focus on the security aspect of working with cloud technologies, which have not yet received adequate coverage in the Ukrainian scientific literature.

The **purpose of the study**. Accordingly, the purpose of this article is to analyze the security factor in the work of organizations with the use of cloud technologies.

Presentation of the basic material of the study. The concept of cloud technology was first used by E. Schmidt, the CEO of Google. However, their very concept emerged back in 1960, at the same time the American researcher J. McCarthy suggested that soon computer computing will be provided akin to public utilities. Consequently, since 2008 the term began to be used en masse in the field of information technology [2, p. 86]. The increase in the use of cloud computing led to the spread of highly powerful networks, the low cost of computerized systems and data storage apparatuses, the spread of virtualization principles, etc.

Modern researchers note that the term cloud technology should be understood as technologies that provide Internet users with access to computer resources of servers and facilitate the use of software as an online service. Consequently, if the user has the ability to connect to the Internet, he can use the mechanisms of complex calculations, to process various kinds of data, while using the power of remote servers [1, p. 41]. The specified technologies allow to manage the organization much more effectively through centralization of the managerial or accounting information, bandwidth, processing, and reliability of data storage. So, the user gets access to personal data but does not have the ability to manage and not worry about the operating system or the software on which he works. At the same time, an important aspect of the use of cloud technology is its cost-effectiveness, which affects the accessibility to different segments of the population in order to preserve information data. Individual organizations use them for work that requires temporary computing, instead of setting up an internal infrastructure [8, p. 12]. This is quite convenient in financial terms since the calculation itself lasts only during the period of their use. At the same time, it should be remembered that the use of cloud technologies can also lead to the risk of loss of information, where the possibility of control is quite limited.

Obviously, public clouds, like other networked systems, can be subject to attacks on the Internet. In general, researchers identify several attacks that may be specific to cloud systems [5, p. 498]:

1. Typical attacks affecting software
2. Attacks that exclusively target the client
3. Network attacks
4. Attacks that primarily target cloud servers
5. Attacks, which carry out a variety of threats.

Despite this, experts note that if a hacker has successfully orchestrated an attack, there is a threat of information security breach over every element of the cloud. In particular, such categories as privacy, confidentiality, and integrity are involved. In addition, a key feature of building a high level of security is providing access to private data to disinterested parties, which is established through additional activity protocols between the user and the cloud system provider.

In general, the system affecting the security of customer information can be exposed to threats such as cross-scripting, phishing, trojans, and viruses. This is due to the fact that, as a rule, consumers, working with cloud computing service, use the Internet browser [9, p. 11]. In order to optimize information security at this level, it is necessary on the client-side to use licensed antivirus software packages, personal firewall tools, tools for encrypting data or information on the disk, and a properly configured Internet browser.

These vulnerabilities point to the importance of protecting cloud platforms, infrastructures, hosted applications, and information and create a demand for top-level cloud security management and centralized security management in cloud environments. Other major concerns for IT managers are the compatibility of the cloud with company policies, IS development environments, and business needs.

There is also the need to properly organize the subsystem responsible for keeping data in the public cloud. It is about keeping it safe, for which a special virtual private network (VPN) tunnel is used

[1, p. 43]. Thanks to this, it is possible to achieve client-server association with the proper level of secure connection.

In addition, the security of virtualization mechanisms also affects the reliability of the virtual environment. For example, if an attack is organized on a virtual machine monitor, then an attacker can edit, copy or block information flow unnoticed by the protection system located in virtual machines. Thus, if a hacker gains access to the control capabilities, he can not only edit the data but also steal across the entire virtual network. Therefore, in order to avoid this situation, it is necessary to protect before administration or virtual machine servers [10, p. 10]. Besides this, it is also necessary to create specialized information protection tools, which can control the traffic inside the necessary server. The replication network transmits segments of their RAM, so if attackers intercept data during an attack, there is a direct security threat, hence it is necessary to isolate the replication network from other networks and use certified VPNs for the replication channel [8, p. 8]. It is not necessary to rely on the triviality of virtual machine structure, as this can lead to great security problems, but it is necessary to organize the process of virtual machine management, so that it is consistent with the organization's security policy.

In addition to the internal software organization, it is worth noting the general provisions of security compliance at cloud facilities. The presence of a video surveillance system allows you to visually monitor everything that happens in the enterprise, its advantages lie in the following: no need to assign separate guards to each server, 24/7 and remote control over the object, the ability to review old records, if necessary, to identify potential and actual intruders is important. For comprehensive data center security, threats such as possible fires or smoke should be considered, and the best effective tools are employee and security notification systems to combat. One of the most effective notification methods is an automated fire extinguishing system, which acts on the fire center while it is still in progress and does not allow the fire to become extensive, which leads to minimization of losses [4, p. 62]. The system of access control and administration allows an automated way to control entrances and exits, limit user access to a certain territory, keep statistics of visitors, monitor the movement of users on the territory, etc. Consequently, compliance with elementary security rules is also important for the safe operation of servers.

Also, the following economic issues can prevent sufficient resistance to virtual threats [6]:

1. Lack of sufficient internal resources - lack of training/education is one of the biggest obstacles to the rapid implementation of security programs in small businesses. Small business owners tend to make decisions without advice from competent IT professionals. These firms often lack experienced IT support staff, and rarely do small business owners deviate from individual decisions to listen to the advice of outside IT professionals. It also happens that small businesses usually don't have the financial resources to hire advanced IT professionals in-house.

2. Lack of time to implement new initiatives - Lack of sufficient time is also a major barrier to the rapid adoption of security systems in small businesses. Small businesses are often understaffed and overworked, leaving very little time to implement new initiatives. While cloud computing can bring significant benefits to small businesses, implementation is often delayed due to a lack of time for firm leaders to even consider the prospect.

3. Cost Management - There are other barriers to rapid adoption - particularly the cost of supporting the cloud and the speed of uploading files. Cloud costs can rise quickly, especially for customizations to meet business needs. Uploading large files can take a long time, creating frustration and inconvenience for day-to-day business operations. Other obstacles include management and control, the complexity of building a private cloud, and performance issues.

4. Cloud control is another obstacle to the rapid introduction of security into online small business operations. The cloud is inherently an open and shared resource. It is a potential target of cyber attackers. The top three cloud security issues facing small businesses are legal issues, compliance, and loss of control over data.

Important benefits, such as increased IT infrastructure flexibility, computing power, the ability to use existing infrastructure with pay-per-use, and the use of that infrastructure to analyze big data, better visibility of information, and the cost-effectiveness of disaster recovery upgrades make cloud technology popular. Servers hosted in the cloud provide significant savings for small businesses. Using PaaS and SaaS structures, small businesses can benefit and improve performance and security [5, p. 500]. This allows the IT infrastructure of small businesses to evolve quickly and allows companies to save time and focus on new opportunities. Small businesses are now able to access the same types of high-quality

enterprise IT services used by larger organizations at a price and scale available to smaller businesses. Small businesses will retain critical company data in a secure cloud-based system. Cloud services are not only less expensive than traditional ways for small businesses to manage internal IT, but they are also secure for data storage and disaster recovery. Small businesses can use the many SaaS-based programs and services available for business project management, document storage and sharing, marketing, and accounting at an affordable price. The study also discussed an example of a small business that successfully transitioned to cloud infrastructure and used various SaaS-based applications and services to reduce operating costs and improve productivity [5, p. 502].

When working with cloud technologies, one should also consider the economic aspects - to treat the security of one's environment responsibly. Cloud computing allows organizations to effectively manage their business. Through cloud computing, you can avoid unnecessary procedural, administrative, hardware, and software costs [8, p. 11]. In the costs of organizations in general, cloud computing allows organizations to effectively manage their business. By means of cloud computing, it is possible to avoid unnecessary procedural, administrative, hardware, and software costs in the expenses of organizations.

Conclusions. The use of cloud technologies when working with information is an important attribute when working with modern networked systems. With all their advantages (convenient access, mobility, and low resource costs), ensuring overall data security is a major challenge. The high risk of hacker attacks and lack of skills when working with server systems can lead to the loss or theft of information that is almost impossible to restore. To optimize information security, the cloud service client must use licensed anti-virus packages and have a properly configured Internet browser. There is also a need to properly organize the subsystem responsible for saving data in the public cloud. We are talking about keeping it safe, for which a special virtual private network (VPN) tunnel is used. At the same time, following basic security rules is also important for secure server operations. When implemented properly, cloud technology has real potential to provide accuracy, reliability, improved service, and cost savings for small businesses. The challenge for IT experts today is to understand the role of the cloud and develop strategies that leverage its potential. They must meet the prerequisites (the steps of a cloud adoption strategy) before making the technology decisions necessary for a service-oriented business.

References

1. Kulyk, V. A. & Liubymov, M.O. (2019). Opportunities, threats, and prospects for using cloud technologies in accounting. *Naukovyj visnyk PUET, 2 (93)*, 40-46.
2. Litoshenko, A.V. (2017). Cloud computing as a kind of outsourcing of Computer Services and its advantages. *Ekonomika ta derzhava, 6*, 86-89.
3. Liubymov, M. O. & Kulyk, V.A. (2019). Opportunities, threats, and prospects for using cloud technologies in accounting. *Naukovyj visnyk Poltavs'koho universytetu ekonomiky i torhivli, 2(93)*, 40-46.
4. Mazina, O.I., Olijnyk, V.S. & Rohoznyj, S.A. (2020), Digitalization as the most important tool for the development of the accounting and reporting system. *Internauka. Seriia: Ekonomichni nauky, 5(37)*, 59-66.
5. Attaran, M., & Woods, J. (2018). Cloud computing technology: Improving small business performance using the internet. *Journal of Small Business & Entrepreneurship, 31(6)*, 495-519. https://doi.org/10.1080/08276331.2018.1466850
6. Cresswell, K., Domínguez Hernández, A., Williams, R., & Sheikh, A. (2022). Key challenges and opportunities for cloud technology in health care: Semistructured interview study. *JMIR Human Factors, 9(1)*, e31246. https://doi.org/10.2196/31246
7. Gleeson, N., & Walden, I. (2021). Cloud computing, standards, and the law. *Cloud Computing Law*, 501-524. https://doi.org/10.1093/oso/9780198716662.003.0015
8. Palos-Sanchez, P. R., Arenas-Marquez, F. J., & Aguayo-Camacho, M. (2017). Cloud computing (SaaS) adoption as a strategic technology: Results of an empirical study. *Mobile Information Systems*, 2017, 1-20. https://doi.org/10.1155/2017/2536040
9. Scale, M. E. (2009). Cloud computing and collaboration. Library *Hi Tech News, 26(9)*, 10-13. https://doi.org/10.1108/07419050911010741
10. Xue, C. T., & Xin, F. T. (2016). Benefits and challenges of the adoption of cloud computing in business. *International Journal on Cloud Computing: Services and Architecture, 6(6)*, 01-15. https://doi.org/10.5121/ijccsa.2016.6601