275. THE DARK SIDE OF CLOUD TECHNOLOGY

Sankevich S.A.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Shevaldysheva E.Z. – Associate Professor

This study analyzes the limitations and potential hazards associated with cloud technologies, such as technical failures, security incidents, and legal challenges arising from data jurisdiction issues. Particular focus is given to the tension between system functionality and user privacy, as well as the necessity for enhanced security measures and the reduction of centralization within cloud environments.

It is a common perception that cloud infrastructure functions solely as an external computational resource, providing enhanced reliability and security compared to on-premises systems. Cloud environments are associated with significant risks that often remain poorly understood by end-users.

The convenience of using cloud technologies is obvious: access from anywhere, scalability, and no costs for your own hardware. However, it is centralization that creates the main problem — dependence on a limited number of companies. When one major provider goes down, thousands of services around the world come to a halt as a result. History knows several high-profile outages of cloud platforms that clearly demonstrate the vulnerability of modern IT infrastructure. Advanced data breaches are difficult to spot. Below are examples of known cases of cloud service failures.

In 2014, Apple is iCloud was hacked, resulting in a massive data leak and many users losing access to their accounts. The attackers obtained celebrities personal photos and messages. Following the hack, Apple implemented a new two-step verification system and improved its cloud security [1]. This new system is still widely used in the financial, legal, and data storage sectors.

In 2019, due to improperly configured cloud storage settings, Microsoft exposed millions of customer support records. The data was stored in Azure is Blob Storage, and it was later discovered that all customer support conversations were publicly accessible, resulting in the loss of a significant amount of sensitive information. This incident was caused by a security configuration issue. Microsoft swiftly responded and protected all customer data, claiming that a third-party company working with Microsoft was responsible for the breach. The company stated that the attackers did not have time to access the data, but the data was publicly available for a short period due to a configuration error. Microsoft quickly resolved the issue and improved the data protection system. To prevent such errors in the future, the developers increased the number of checks and implemented new security protocols for cloud storage [2].

Technical failures are not the only problem. The legal aspects, which users often do not think about, are equally important. The largest cloud providers are American companies, and they are subject to US legislation, in particular the Cloud Act. This law allows US intelligence agencies to request access to the data of any American company, no matter where the servers are physically located. Several Belarusian firms retain data within European jurisdictions while relying on servers operated by American service providers. Although this data is generally protected under European legal frameworks, requests from the FBI can compel these providers to grant access to the data without informing or obtaining consent from the data owners.

Nowadays, end-to-end encryption is actively used to avoid data leaks. When it is used, only the owner can access the data. However, companies do not often use this system because it hinders data analysis for improving the service. In this regard, the demand for «zero-knowledge» services is growing, where the company technically cannot decrypt customer data. This creates a contradiction between the convenience of the functionality and the privacy of the user.

Even without government intervention, the provider itself has the technical ability to view user data. User agreements often allow companies to scan content to improve services, train neural networks, or target advertising. Technically, the cloud administrator has physical access to the servers, and even encryption does not always help if the keys are stored in the same place. In this situation, the user cannot know who is viewing their data and for what purpose. It allows people from anywhere in the world to access their data and not depend on physical storage media.

Cloud service security is currently a top priority for companies. Companies need to allocate resources not only to developing new technologies but also to making them secure. It is also necessary to establish an international jurisdiction that would allow people, regardless of their location, to access their data and not fear that in another country they will be unable to do so. Centralization should also be reduced so that in the event of failures, there are no severe disruptions and a huge number of people do not lose their data all at once. Cloud technologies are undoubtedly a useful tool, which, however, needs to be significantly improved.

References:

1. Cloud Computing News: [website] / TechForge Media Ltd. – London, 2025. – URL: https://www.cloudcomputing-news.net/news/10-real-life-cloud-security-failures-and-what-we-can-learn-from-them/ (date of access: 18.03.2025).

2. Electronic Specifier: [website] / Electronic Specifier Ltd. – London, 2020. – URL: https://www.electronicspecifier.com/industries/robotics/the-biggest-cloud-breaches-of-the-decade/ (date of access: 18.02.2020).