3. *Що таке інтерфейс користувача та як він впливає на продажі | Wezom*. (n.d.). IT-компания полного цикла разработки программных продуктов WEZOM - Киев, Украина. https://wezom.com.ua/ua/blog/chto-takoe-ui-i-kak-polzovatelskij-interfejs-vliyaet-na-prodazhi-internet-magazina

4. *Colors in UI design: A guide for creating the perfect UI - usability geek*. (n.d.). Usability Geek. https://usabilitygeek.com/colors-in-ui-design-a-guide-for-creating-the-perfect-ui/#:~:text=The%20right%20color%20selection%20always,fulfill%20subconscious%20aesthetic%20user%20needs

5. Opatsa, V. (2023, August 3). *Кольорова психологія в дизайні інтерфейсу та брендингу*. UXPUB UA Дизайн-спільнота. https://ux.pub/vio/kolorova-psikhologhiia-v-dizaini-intierfieisu-ta-briendinghu-220c

6. *Understanding colors for UI/UX design: A comprehensive guide*. (n.d.). Taking Digital Forward | QED42. https://www.qed42.com/insights/coe/design/understanding-colors-ui-design#:~:text=While%20using%20the%206:3,one%20point%20to%20another%20comfortably

Tetiana Liubchenko

Kyiv National University of Technologies and Design (Kyiv)

Scientific supervisor – senior lecturer Natalia Liubymova

RESEARCH AND DEVELOPMENT OF CRYPTOGRAPHIC METHODS FOR INFORMATION SECURITY IN CLOUD COMPUTING

The research and development of cryptographic methods for information security in cloud computing is a relevant and important area of information security in light of the rapid development of technologies and the widespread use of cloud resources. In this context, overcoming new challenges and threats related to the

transmission and storage of confidential information in cloud environments is the most important task for modern cryptographers and information security experts.

In the modern world of globalization, most information is available on the Internet or on web resources, so newer and more modern encryption methods need to be used. Cloud computing seemed like the future, but it has already become a necessary part of the modern information landscape. Thanks to the ability to access computing resources and store data over the Internet, it has become an important tool for users and businesses. However, the growing popularity of cloud computing leads to an increase in information security threats [1]. Therefore, the research and development of cryptographic methods to protect information in cloud computing is becoming an urgent task.

Before studying cryptographic methods of protecting information in cloud computing, it is important to understand the basic principles of this technology. Cloud computing is based on the following principles:

Virtualization: This principle consists in representing computing resources, networks, and data storage as virtual, which allows you to allocate and manage resources more efficiently. Virtualization can be used to create virtual servers, networks, and even virtual cloud computing infrastructures [2].

Scalability: Cloud computing can easily increase or decrease computing resources depending on the needs of the user. This allows businesses to respond effectively to changes in workload and scale their services without significant costs.

Availability: This principle means that the information and resources hosted in cloud computing are accessible from anywhere in the world with an Internet connection. This makes work more flexible and convenient for users.

Cloud computing can be provided in three main service models:

Infrastructure as a Service (IaaS): Users receive basic computing resources, such as processors and storage devices, and use them to create their own operating systems and applications. The consumer does not manage the basic cloud

infrastructure, but has control over operating systems, storage systems, and deployed applications. Limited control over the choice of network components is possible (for example, a host with firewalls).

Platform as a Service (PaaS): Users can install their own applications on a platform provided by a service provider. The user does not manage the underlying cloud infrastructure: networks, servers, operating systems, and storage systems, but has control over the deployed applications and some configuration parameters of the hosting environment.

Software as a Service (SaaS): Not only data is stored in the cloud, but also related programs, and the user only needs a web browser to work. The consumer uses the applications of a provider operating in the cloud infrastructure. At the same time, the user does not manage the underlying cloud infrastructure - networks, servers, operating systems, storage systems, even individual application settings, except for some application configuration settings.

Currently, three giants rule the world - AWS, Azure, and Google Cloud. These companies occupy the lion's share of the market around the world (except for China, there is also Alibaba Cloud), are technological leaders and set trends in the development of cloud IaaS services. For example, AWS currently has more than 100 services in its portfolio (IaaS, SaaS, PaaS).

Thanks to cloud computing, an organization's data can be analyzed to find patterns and information, make forecasts, improve them, and make other business decisions. Cloud services can provide your organization with higher computing power and advanced tools for retrieving huge amounts of data, as well as the ability to quickly scale your environment as your data grows [3].

Cryptographic methods of protecting information are special methods of encrypting, coding, or otherwise transforming information, because of which its content becomes inaccessible without presenting the cryptogram key and reverse transformation.

Various cryptographic methods are used to ensure security in cloud computing:

Data encryption: Encryption is one of the key components of security in cloud computing. Strong encryption algorithms such as AES, RSA, or ECC are used to protect data privacy. This method provides encrypted storage and transmission of information, so that even if the data is illegally accessed, attackers cannot read or use the information without proper decryption.

Electronic signature: An electronic signature system is a cryptographic transformation attached to a text that allows another user to verify the authorship and authenticity of a message when it is received by another user. This method allows users to determine whether data has been altered during transmission or storage.

Multifactor authentication: Multifactor authentication requires users to provide not only a password or login, but also additional types of identification, such as fingerprints, one-time passwords, or smart cards. This method increases the security of access to cloud resources and makes it more difficult to gain access even if a stolen password is used [4].

Key exchange: Securing encryption keys is critical to ensuring security in cloud computing. Encryption keys must be stored in secure containers and exchanged between parties in a secure manner. Techniques such as key exchange protocols and key management systems play an important role in ensuring that cryptographic protection in cloud computing is robust.

These cryptographic techniques are an integral part of the security strategy in a cloud computing infrastructure and help ensure the confidentiality, integrity, and availability of data and services.

The main areas of use of cryptographic methods are the transmission of confidential information through communication channels (e.g., e-mail), authentication of transmitted messages, and storage of information (documents, databases) on encrypted media.

To overcome these threats and ensure security in cloud computing, it is important to continue researching and developing new cryptographic methods. Scientists and engineers are actively working on the development of quantum cryptography, which can become a new standard in cloud computing security.

Cloud computing provides many opportunities, but also brings threats to information security. The development and implementation of effective cryptographic methods is an important task for ensuring security in cloud computing. Continuous research and innovation in this area will help ensure the confidentiality, integrity, and availability of information in cloud services in the future.

Thus, the choice of the type of cryptographic security implementation for a particular IS depends to a large extent on its features and should be based on a comprehensive analysis of the requirements for the information security system.

REFERENCE

1. *Тема: Криптографічні методи захисту інформації. контроль цілісності програмних і інформаційних ресурсів.* (n.d.). Освітній проект «На Урок» для вчителів. https://naurok.com.ua/tema-kriptografichni-metodi-zahistu-informaci-kontrol-cilisnosti-programnih-i-informaciynih-resursiv-210574.html
2. Lazo, L. G. D., & Kumar, D. P. V. S. (2022). Role and importance of cryptography techniques in cloud computing. *Technoarete Transactions on Internet of Things and Cloud Computing Research*, *2*(2). https://doi.org/10.36647/ttitccr/02.02.art005
3. *Classmill - 11 клас Інформатика*. (n.d.). Classmill - Create classes with links, videos, images & files. https://classmill.com/659/112/m/xnb7A
4. *Що таке хмарні технології? Переваги та недоліки хмарних сервісів | EDIN*. (n.d.). EDIN. https://edin.ua/shho-take-xmarni-texnologiї-i-navishho-voni-potribni/