Section 1

ONLINE BANKING INFORMATION SECURITY

Heorhii Zemlianko
National Aerospace University «Kharkiv Aviation Institute»
Scientific advisor: Vyacheslav Kharchenko

Relevance. In today's reality, the state of information security in online systems has become a global concern. In fact, the spread of cybercrime has transcended geographical boundaries and has become a critical international issue. It is noticeable that the fragile state of information security in financial institutions makes them increasingly vulnerable to potential cyber-attacks, which has raised alarm bells in the expert community [1].

There are numerous examples of online systems being disrupted. Intellectual property theft, for example, has become an alarmingly common occurrence in the digital world. Despite the universal nature of such incidents, banking institutions are still reluctant to publicly acknowledge such breaches. This reluctance is due, at least in part, to the profound impact that such admissions can have on customer confidence, which further complicates the situation.

Even in countries where e-business is at its peak, the volume of financial transactions conducted online is significantly limited. In practice, these transactions tend to involve relatively small amounts of money. This phenomenon is largely due to a lack of attention to information security in the complex environment of electronic systems [2].

A close analysis of the available data reveals a complex interaction between information security and the conduct of online business. For example, there have been numerous instances of major hacks and data breaches that have severely impacted organizations and limited their ability to conduct high-value financial transactions. These incidents are prime examples of deep information security issues.

Purpose. This study aims to comprehensively address key issues in the security of online banking systems by examining various aspects of information security. It aims to understand and evaluate the challenges faced by online systems in securing financial data and transactions. The research seeks to provide insights and recommendations to improve security measures in online banking. By analyzing emerging threats and technologies, it aims to provide a robust framework for protecting this critical financial infrastructure in the evolving digital landscape.

Principal provisions. Therefore, the issue of protecting online banking systems is of paramount importance in their development and operation. and operation. Information in online systems must be protected. At the same time, the cost of organizing protection should not exceed the losses that may arise from a breach of the protection system for the entire period of system operation. In addition, any elements of the protection system should not reduce the reliability of the on-line banking system.

An adequate level of information security of an on-line system is particularly relevant for open public systems that process classified information with limited access. After all, all devices and processes of the system (computer network) interact with each other according to a certain set of standards and are open to interaction with other systems (computer networks). This is due to the need to involve a large number of systems, a large number of technical means, and programs used in computer systems or networks. Therefore, a computer system that conforms to certain standards will be open to certain standards, will be open to interconnection with any other system that conforms to the same standards. This also applies to mechanisms for cryptographic protection of information or protection against unauthorized access to information.

Conclusions. Thus, the development of trends in the processing of banking information on the basis of modern automated technologies and the constant increase in the number of users of on-line systems are accompanied by the emergence of new threats, which are negative companions of scientific and technological progress. Therefore, the development of the security system of the on-line banking system should include the creation of a model of possible threats and the selection of effective security methods, which, in turn, should be an integral part of the on-line banking system at all stages of its operation.

List of references

1. Krebs on Security – In-depth security news and investigation. *Krebs on Security – In-depth security news and investigation*. URL – https://krebsonsecurity.com/ (date of access: 01.10.2023);
2. Scritube – publica fisierul tau pe internet, articole, documente, informatii online. *Scritube - publica fisierul tau pe internet, articole, documente, informatii online*. URL – https://www.scritub.com (date of access: 01.10.2023);
3. Як еволюціонує мобільний банкінг у світі та чому українські необанки на крок попереду. *PaySpace Magazine*. URL: https://psm7.com/ru/fintech/kak-evolyucioniruet-mobilnyj-banking-v-mire-i-pochemu-ukrainskie-neobanki-na-shag-vperedi.html (date of access: 01.10.2023).

Information about the authors

Heorhii Zemlianko, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», g.zemlynko@student.csn.khai.edu
Vyacheslav Kharchenko, Dr. Sc., professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.kharchenko@csn.khai.edu