The development of electronic payment systems in Ukraine and their security

Liudmyla Polovenko[*] [A]; Svitlana Merinova [B]; Kateryna Kopniak [C]

[A, B, C] Vinnytsia Institute of Trade and Economics of Kyiv National University of Trade and Economics, Soborna st., 87, UA-21050, Vinnytsia, Ukraine

Received: April 20, 2021 | Revised: May 28, 2021 | Accepted: June 19, 2021

JEL Classification: E42, L14, L81, L86.

DOI: 10.38188/2534-9228.21.2.17

Abstract

The paper is devoted to the study of innovations in the market of modern payment systems. The pandemic and quarantine restrictions have accelerated the expansion of the payment infrastructure in Ukraine, which in turn raises the issue of security of electronic payment systems. Ukrainians are more actively switching to electronic payments. At the same time, the trend of growing popularity of contactless payment instruments and settlements with them continues. A comparative analysis of the security of payment systems using electronic technologies in the implementation of money transfer services in Ukraine has been performed. The components of the payment system, information security measures in the electronic payment system have been also considered. The schema of electronic payments and the block diagram of the information protection subsystem of electronic payment system have been constructed. The criteria for assessing the security of the electronic payment system have been determined. A total of fifteen safety criteria have been identified, they are divided into six groups according to the degree of safety. Six electronic system payments were used for the study and the research results have been presented in this paper. The tendencies of development of electronic payment systems in modern conditions and ways of improvement of their activity taking into account the newest information technologies have been outlined.

Keywords: electronic payment system, internet banking, vulnerabilities, security of payment systems, non-cash payment instruments.

Introduction

In today's world, settlements between economic agents are impossible to imagine without the use of payment systems. In the digital economy, ubiquitous access to communication channels, as well as the rapid development of new information technologies, the rapid spread of new payment methods, the emergence of alternative devices used, increasing demands on the development of electronic payment systems. This trend not only forces payment system operators to constantly improve payment services, but also raises questions about the effective security of electronic payment systems.

There are two serious problems – unauthorized debiting of funds from bank cards or accounts of legal entities and the general guarantee of preservation of payments made through non-bank payment transfer systems.

[*] **Corresponding author:**

[A] PhD, Associate Professor, Department of Economic Cybernetics and Information Systems, e-mail: l.polovenko@vtei.edu.ua, ORCID: 0000-0002-9909-825X

[B] PhD, Associate Professor, Department of Economic Cybernetics and Information Systems, e-mail: s.merinova@vtei.edu.ua, ORCID: 0000-0001-6563-5320

[C] Senior Lecturer, Department of Economic Cybernetics and Information Systems, e-mail: k.kopniak@vtei.edu.ua, ORCID: 0000-0003-0618-0359

Material and methods

During the work were used: system method, which allows investigating the development of electronic payment systems; methods of analysis and synthesis, induction and deduction (to assess the degree of security of the studied payment systems), systematization, logical approach, grouping and generalization.

The analysis of previous researches on the corresponding subjects is carried out. In particular, the research which devoted to the study of the essence and types of payment systems is taken as a basis (Balakina, 2019). The study of I. Harper, R. Simes and C. Malam is devoted to the development of retail electronic payment systems, in particular, in Australia (Harper et al., 2006).

The problem of information security in the system of electronic payments was studied by V. Akhramovich and V. Chegrenets. Researchers consider the technology of building an information security management system and features of information security management in banking institutions (Akhramovich and Chegrenets, 2019).

Prospects for the development of the electronic payment system are demonstrated in the work of I. Kravchenko and I. Drozd (Kravchenko and Drozd, 2014).

The pandemic and quarantine restrictions have accelerated the expansion of the payment infrastructure, which in turn raises the issue of security of electronic payment systems (National Bank of Ukraine, 2020).

The object of research is the process of functioning of electronic payment systems and the formation of a security system. The subject of the study is electronic payment systems.

Results and discussion

1. Innovations in the market of modern payment systems

Currently, customers of the payment system mostly switch to the latest technology of Internet banking. The basis for improving customer service technology has become not just a form of i-Banking, but mobile banking. This innovation, thanks to the purchase for private use of smartphones with flexible and secure Microsoft technologies, as well as the iPad is a model of a comprehensive remote service solution, which includes Internet banking, mobile banking and a portal for personal provision of various, including confidential, services with more 200 built-in templates for financial transactions and maintenance of virtual customer accounts.

Mobile applications allow not only checking the balance of personal finances, but also to carry out account replenishment operations, remotely making utility payments and purchases in online stores and other commercial structures.

"Design" technologies in traditional banking structures or other credit institutions, special web portals and mobile device applications create a tendency to abolish commercial banks unnecessarily. Investment borrowing in this case takes the form of contractual and paid crowd funding, i.e. "public borrowing" to lend to projects that inspire confidence in private creditors.

A trend is formed, expressed by the formula: "banks must go, long live banking", and the agreement on borrowing funds is based on a mobile P2P-platform.

The term "electronic payment system" (EPS) means a system of settlements in which payments are made via Internet channels, the traditional processing of payment orders does not occur (Balakina, 2019).

This definition includes:

- bank card payments of traditional Visa, MasterCard, American Express and Diners Club systems. Here, with an absolute guarantee of transaction protection, there is a problem of unauthorized write-offs as a result of intercepting traffic or obtaining card numbers;
- programs of interbank settlements via electronic communication channels, including

fast payments made by banks by telephone numbers;

- payments through electronic wallets (Google Pay and others).

The market of electronic payment systems in Ukraine today can be confidently called developing – in this area so far with some success operating about 10 systems.

The first to be mentioned are national payment systems, such as: Electronic Payment System (EPS) and "Ukrainian Payment Space".

Portmone (credit payment scheme provides electronic delivery and payment of bills with Visa, MasterCard), LiqPay (PrivatBank payment system), Wayforpay, Welsend, Telegraf, Google Pay and others can be called successful in the Ukrainian market.

However, the introduction of innovative technologies of modern Internet banking, electronic payment systems is associated with a high risk of data theft. Therefore, it is worth paying attention to the security of electronic payment systems.

2. Security of electronic payment systems

If we talk about protection against unauthorized transfers of EPS in general, then regardless of the level of each specific model, they have the same requirements.

Among the most vulnerable places:

- Internet traffic between participants in the exchange of electronic messages about financial transactions (banks, payment wallet operators, ATMs, customers);
- information processing within the bank or operator, when the data may be available to employees;
- constant availability of payment systems for customers, no failures in their work and on the communication line.

The presence of these vulnerabilities forces banks and operators to protect traffic when forwarding in accessible ways (transmission over secure channels, encryption) and to develop authentication models for sender and recipient.

At the same time in the work of the bank or payment operator there are problems:

- determining the mutual authenticity of the participants in the transaction when establishing a connection;
- ensuring the confidentiality and authenticity of payment orders sent via the Internet and other documents;
- protection of the sending process, formation of evidence of sending and receiving documents;
- ensuring the execution of the document (for example, the permanent presence of the balance on the correspondent account of the bank, which allows you to arrange payment).

The Bank and the EPS operator are obliged to implement mechanisms to protect customers from unauthorized write-offs, specific requirements for which are determined by the policies of operators and regulations of the NBU:

- management of access of the client, employees of the operator and the recipient, creation of the authentication mechanism;
- control of reliability and integrity of information in the message;
- ensuring the confidentiality of information in the transmission process;
- inability to refuse the authorship of a power of attorney to send funds or a notice;
- guarantees of access to resources and loss of the message in the course of its delivery;
- inability of the operator or bank to refuse to execute the order for transfer or payment;
- saving data on orders and messages.

On the basis of the national EPS payment system, consider the system of EPS (Fig. 1).

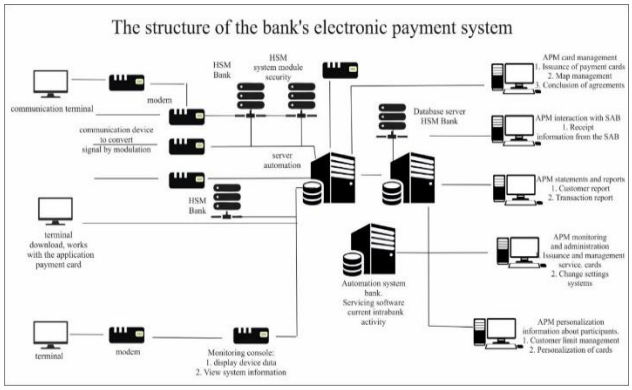

Fig.1. Block diagram of electronic payments

The information security of this system is controlled by the bodies of the Security Department and is performed in accordance with the provisions on the protection of electronic banking documents using the means of information protection of the National Bank of Ukraine (NBU).

Technological means of control built into the software and hardware systems of EPS cannot be disabled. In case of detection of an unusual situation, which may indicate a suspicion of unauthorized access to EPS on behalf of a particular EPS participant, processing center of EPS automatically stops accepting initial electronic settlement documents and notifications from this participant. The main means of encrypting files (packages) EPS is cryptographic information protection equipment (CIPE).

The work of CIPE is controlled by the software means of information protection built in processing center of SEP and automated workplace of SEP (AWP-SEP) and provides hardware encryption (decryption) of the information according to the algorithm defined in the National standard of Ukraine DSTU 28147:2009. As a backup means of encryption in EPS the built-in function of software encryption built in processing center of SEP and AWP-SEP is used.

Processing center of SEP and AWP-SEP encryption tools (both CIPE and software encryption) provide strict authentication of the sender and recipient of an electronic banking document, the integrity of each document as a result of the impossibility of forgery or unauthorized modification in encrypted form. Workstation-SEP and processing center of SEP in real time provide additional strict mutual authentication when establishing a communication session. During the work of AWP-SEP creates logs of software and hardware encryption and protected from modification work protocol of AWP-SEP, which records all actions performed by it, indicating the date and time of processing of electronic banking documents. At the end of the banking day, the logs of software and hardware encryption and the protocol of the workstation-EPS are subject to mandatory storage in the archive (Akhramovich and Chegrenets, 2019).

The Security Department provides banks (branches) with information services on the accuracy of information on electronic banking documents in the event of disputes based on a copy of the archive of the workstation-workstation for the relevant banking day.

The Security Department decrypts a copy of this archive and identifies:

1) the identifier of the bank – EPS participant, which sent (encrypted) the electronic banking document;

2) the identifier of the bank – EPS participant to which the electronic banking document is addressed;

3) date, hour and minute of encryption of the electronic banking document;

4) date, hour and minute of decryption of the electronic banking document;

5) compliance of all electronic digital signatures with which the electronic banking document was protected from modification.

When using CIPE, the following are additionally determined:

1) CIPE number on which the encryption or decryption of the electronic banking document was performed;

2) the number of the smart card used during encryption or decryption of the electronic banking document.

The Security Department provides services for decryption of information on electronic banking documents, if there are disputes between EPS participants on issues related to electronic banking documents, in the case of:

1) failure to authenticate or decrypt an electronic banking document;

2) refusal to receive an electronic banking document;

3) waiver of the fact of formation and sending of an electronic banking document;

4) a statement that the recipient received an electronic bank document, but in fact it was not sent;

5) a statement that the electronic banking document was generated and sent, but it was not formed or another message was sent;

6) the occurrence of a dispute regarding the content of the same electronic banking document, formed and sent by the sender and received and correctly authenticated by the recipient;

7) work with the archive of work of AWP-SEP during audits, etc. (Akhramovich and Chegrenets, 2019).

The block diagram of the information protection subsystem in EPS is shown in Fig. 2.

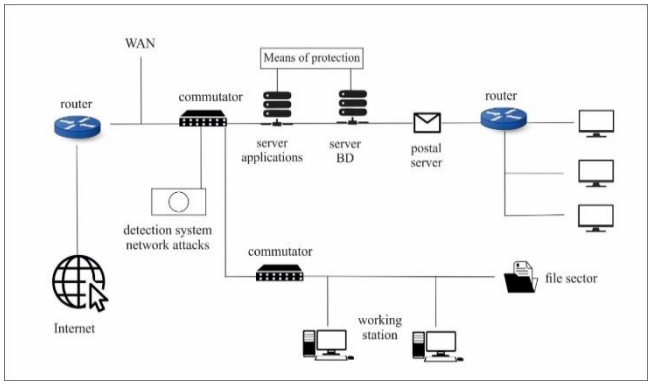

Fig. 2. Block diagram of the information protection subsystem in EPS

In the course of the work, certain criteria for assessing the protection of the EPS were determined (Table 1).

Tab. 1. Safety criteria and sub-criteria

Safety criteria and sub-criteria	
1. Primary protection of the EPS account	
Password protect account (Criterion 1)	
Presence of account password	
Password strength	Minimum 1 character
	Minimum 5-6 characters
	Minimum 8 characters
	The presence of add conditions (special symbols, uppercase, numbers)
The presence of the password security string	
Limited validity of EPS password	
Using a secure connection to a website (Criterion 2)	
SSL connection security	SSL encryption is not used
	SSL encryption is used, but there is unsecured content, with a serious threat
	SSL encryption is used, but there is unsecured content
	SSL encryption is used
The protocol used	TLS 1.1 protocol
	With TLS 1.2
2. Security at authorization in EPS	
Confirmation of login via mobile phone, E-num or e-mail service (Criterion 3)	Mobile phone
	E-num service
	E-mail
3. Authorization using technical settings	
A. Possibility of limited access by IP address (Criterion 4)	
Б. Issuance of a personal digital certificate for access to the EPS (Criterion 5)	
4. Confirmation of operations with a password	
Confirmation of operations (Criterion 6)	SMS
	E-num. Google Authenticator
	With an additional payment password
5. Additional methods and techniques that ensure the security of money	
Ability to link mail, phone to EPS (Criterion 7)	
Possibility to issue or purchase a virtual card with a short validity period or a limit of funds (Criterion 8)	
Presence of identification with confirmation of user documents (Criterion 9)	
Use of secret questions or secret word (Criterion 10)	
Session limitation – automatic logout (Criterion 11)	

6. Information methods of security	
Informing the SMS user about the operations performed (Criterion 12)	
Availability of a log of visits by the EPS user (Criterion 13)	
Availability of safety instructions and recommendations for EPS users (Criterion 14)	
Availability of support service (Criterion 15)	By phone
	By e-mail

If any method or security capability is missing, the security value of this criterion will be equal to 0%. In sum, all criteria give a safety rating of 100%. The security rating of the system depends on the number of collected percentages out of 100. Grade A (excellent) – from 90% (inclusive) and above, grade B (good) – from 80% (inclusive) to 90%, grade C (satisfied) – from 70 % (inclusive) to 80%, grade F (unsatisfactory) – results less than 70%.

A total of 15 safety criteria have been identified, they are divided into 6 groups according to the degree of safety.

For example, in the first subgroup of the first criterion – password protection of the account, where the sub-criteria are the presence of a password, password strength (minimum password starts from 1, 5, 8 characters, or additional characters must be entered), the presence of a password string, password limitation (for example, a few months). The second criterion in the group is a secure connection of websites, where the sub-criteria are the security of SSL connections (if SSL encryption is used and there is unsecured content on the web page), the second sub-criterion is the protocol used (TLS 1.1 or 1.2, in which does not use dangerous encryption algorithms).

6 electronic system payments were used for the study.

The research results are presented in Table 2.

Tab. 2. Protection of electronic payment systems

№	Electronic payment system	Criteria															
		Protecting EPS accounts with password		Security when logging in to EPS	Automation with technical settings		Confirmation of operations with a password	Additional methods and techniques						Information methods of security			Evaluation of all indicators
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	EPS	25	20	5	5	0	0	3	0	3	3	3	3	3	3	6	B – 82%
2	Master-Card	15	20	0	5	5	5	3	3	3	3	3	3	3	3	6	B – 80%
3	GooglePay	25	20	5	5	5	0	0	3	3	0	3	0	3	0	6	C – 73%
4	Portmone	18	20	0	0	0	5	3	0	3	0	3	3	3	0	6	C – 72%
5	LiqPay	20	15	5	0	0	5	3	0	3	3	3	3	3	0	6	F – 69%
6	Telegraf	10	20	0	0	0	5	3	3	3	0	3	3	0	0	6	F – 56%

The study showed that only two EPS – EPS and MASTERCARD – have a rating of “good” (B). Two EPS (GooglePay, Portmone) were rated “satisfactory” (C). All other EPS were assessed as “unsatisfactory”.

3. Development of the electronic payment systems market during the pandemic

Over the last year, there have been rapid changes in citizens' payment habits towards non-cash payments, in particular on the

Internet. Ukrainians are more actively switching to electronic payments. At the same time, the trend of growing popularity of contactless payment instruments and settlements with them continues.

The total number of transactions made with the help of e-commerce for the nine months of 2020 amounted to 4310.2 million units, and their amount – 2807.9 billion UAH. The number of these transactions increased by 18.0%, and the amount – by 8.7% compared to the same period in 2019. The number of non-cash transactions is even higher – 86 out of 100 payment card transactions were carried out non-cash during the nine months of this year. At the same time, the number of transactions for receiving cash from payment cards decreased by 11.3%, and the amount – by 3.3% compared to the first nine months of 2019. Also, during the year, the distribution of non-cash transactions with payment cards by amount changed significantly. Analysis by their types shows that in January-September 2020, the share of Internet transactions increased to almost 30% of the total of all non-cash transactions made with payment cards. For 9 months of 2019, this figure was 27% (National Bank of Ukraine, 2020).

Conclusions

As the level of banking transactions through electronic payment systems has increased significantly over the last year, it is necessary to be careful in choosing a system for payment. For electronic payments, it is recommended to use EPS, which received a rating of "satisfactory" and above, but provided that the user will follow the instructions and recommendations of EPS. Every electronic banking system tries to protect its customers from fraud and, unfortunately, many customers do not follow the recommendations, and therefore fall into the hands of fraudsters.

References

Akhramovich, V.M. & Chegrenets, V.M. (2019). Information bank risk management of a commercial bank. Modern information protection. №2 (38), pp. 54-59. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2317.

Balakina, Yu.S. (2019). Oversight of payment systems in Ukraine. [abstract of the candidate's dissertation, SHEI "University of Banking"]. URL: http://ubs.edu.ua/images/2017/Avtoreferats/kandidat_balakina.pdf.

Ian Harper, Ric Simes & Craig Malam (2006). The Development of Electronic Retail Payments Systems. The Economics of Online Markets and ICT Networks. pp. 25-40. URL: https://www.researchgate.net/publication/226602427_The_Development_of_Electronic_Payments_Systems.

Kravchenko, I.S. & Drozd, I.V. (2014). Current state and prospects of development of the National system of mass electronic payments on the market of bank payment cards in Ukraine. Bulletin of the University of Banking of the National Bank of Ukraine. № 2 (20), pp. 141-148.

National Bank of Ukraine (November 3, 2020). Undeniable Card Market Trends in 2020: Online Settlements and Contactless Payments. URL: https://bank.gov.ua/ua/news/all/bezzaperechni-trendi-kartkovogo-rinku-u-2020-rotsi--rozrahunki-v-interneti-ta-bezkontaktni-plateji