Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2021

UDC 004.01/08

Editorial board:

Black Sea Science 2021: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2021. – 526 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2021» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Sergii Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0" of Odessa National Academy of Food Technologies (Ukraine)

Members of the jury:

Piotr Artiemjew - Dr hab., Associate Professor in Decision Systems of the Faculty of Mathematics and Computer Science,University of Warmia and Mazury in Olsztyn (Poland)

Francisco Antonio Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse "Angel Kanchev" (Bulgaria)

Degla Gérard Hugues – Communications and Training Manager of "MAPCOM solutions informatiques" company group (Benin)

Nugzar Kereselidze - Academic Doctor of Informatics (Computer Science), Associate Professor of the Department of Natural Sciences, Mathematics, Technology and Pharmacy, Sukhumi State University (Georgia)

Etibar Seyidzade - Associate Professor of the Department of Computer and Information Technolohies, Baku Engineering University (Azerbaijan)

Vladimir Golenkov, D.Sc., Professor of the Department of Intelligent Information Technologies, Belarusian State University of Informatics and Radio Electronics (Belarus)

Zhanar Omirbekova - Ph.D., Associate Professor of the Department of Automation and Management, Satbayev University (Kazakhstan)

Ivan Palov - D.Sc., Professor of the Department of Power Supply and Electrical Equipment, University of Ruse "Angel Kanchev" (Bulgaria)

Siarhei Palavenia - Ph.D., Associate Professor, Head of the Department of Telecommunication Systems, Belarusian State Academy of Communications (Belarus)

Alexander Goloskokov - Ph.D., Professor of the Department of Software Engineering and Information Technology Management, National Technical University "Kharkiv Polytechnic Institute" (Ukraine)

Peter Nikolyuk - D.Sc., Professor of the Department of Computer Technology, Vasyl Stus Donetsk National University (Ukraine)

Vladimir Palagin - D.Sc., Professor, Head of the Department of Radio Engineering, Telecommunications and Robotics Systems, Cherkasy State Technological University (Ukraine)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Fedir Trishyn - Ph.D., Associate Professor, Vice-Rector on Scientific and Educational Work, Odessa National Academy of Food Technologies (Ukraine)

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies (Ukraine)

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Anatoly Galiulin - Ph.D., Associate Professor, Acting Head of the Department of Electromechanics and Mechatronics, Odessa National Academy of Food Technologies (Ukraine)

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

DEVELOPMENT OF ELECTRONIC PAYMENT SYSTEMS AND SECURITY OF THEIR FUNCTIONING

Author: ***Anna Severenchuk***
Adviser: ***Lyudmila Polovenko***
Vinnytsia Trade and Economic Institute KNTEU (Ukraine)

Abstract. The work is devoted to the study of innovations in the market of modern payment systems. A comparative analysis of the security of payment systems using electronic technologies in the implementation of money transfer services in Ukraine. The components of the payment system, information security measures in the electronic payment system are also considered and the criteria for assessing the security of the electronic payment system are determined. 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 are outlined.

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

I. 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.

II. ANALYTICAL REVIEW OF LITERATURE

Balakina's work is devoted to the study of the essence and types of payment systems [2].

The problem of information security in the system of electronic payments was studied by Akhramovich, VM Chegrenets [1]. Researchers consider the technology of building an information security management system and features of information security management in banking institutions.

Prospects for the development of the electronic payment system are demonstrated in the work of I.S. Kravchenko, IV Blackbird [3].

The pandemic and quarantine restrictions have accelerated the expansion of the payment infrastructure [4], which in turn raises the issue of security of electronic payment systems.

III. OBJECT, SUBJECT AND METHODS OF RESEARCH

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 are electronic payment systems.

Research methods. During the work were used: system method, which allows to investigate 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.

IV. RESULTS OF WORK

4.1. 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 to check the balance of personal finances, but also to carry out account replenishment operations, remotely make 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, ie "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 [2].

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 (GooglePay 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.

4.2. 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).

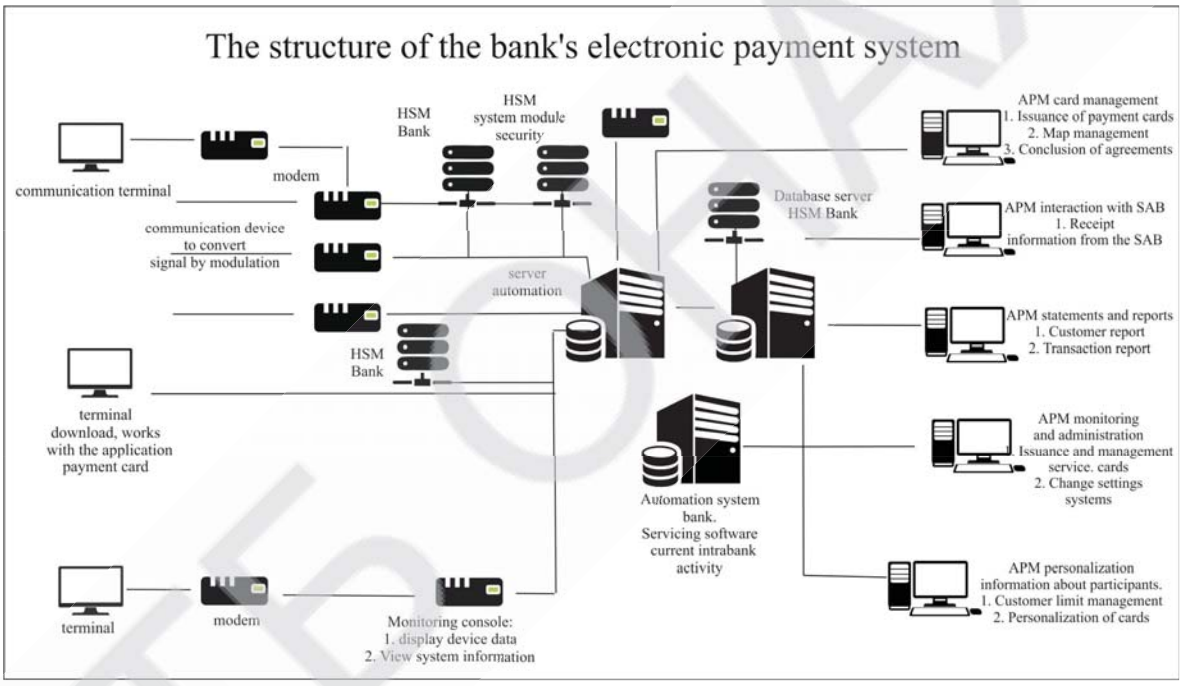

Fig.1. Block diagram of electronic payments

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.

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 susFigion of unauthorized access to EPS on behalf of a particular EPS participant, COSEP automatically stops accepting initial electronic settlement documents and notifications from this participant. The main means of encrypting files (packages) EPS is AKZI. The work of AKZI is controlled by the software ZZI built in TsOSEP and ARM-SEP and provides hardware encryption (decryption) of

the information according to the algorithm defined in the national standard of Ukraine DSTU GOST 28147: 2009. As a backup means of encryption in EPS the built-in function of software encryption built in TsOSEP and ARM-SEP is used. COSEP and ARM-SEP encryption tools (both AKZI 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 COSEP in real time provide additional strict mutual authentication when establishing a communication session. During the work of ARM-SEP creates logs of software and hardware encryption and protected from modification work protocol of ARM-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 [1].

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 AKZI, the following are additionally determined:

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

2) the number of the IC 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 ARM-SEP during audits, etc. [1].

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

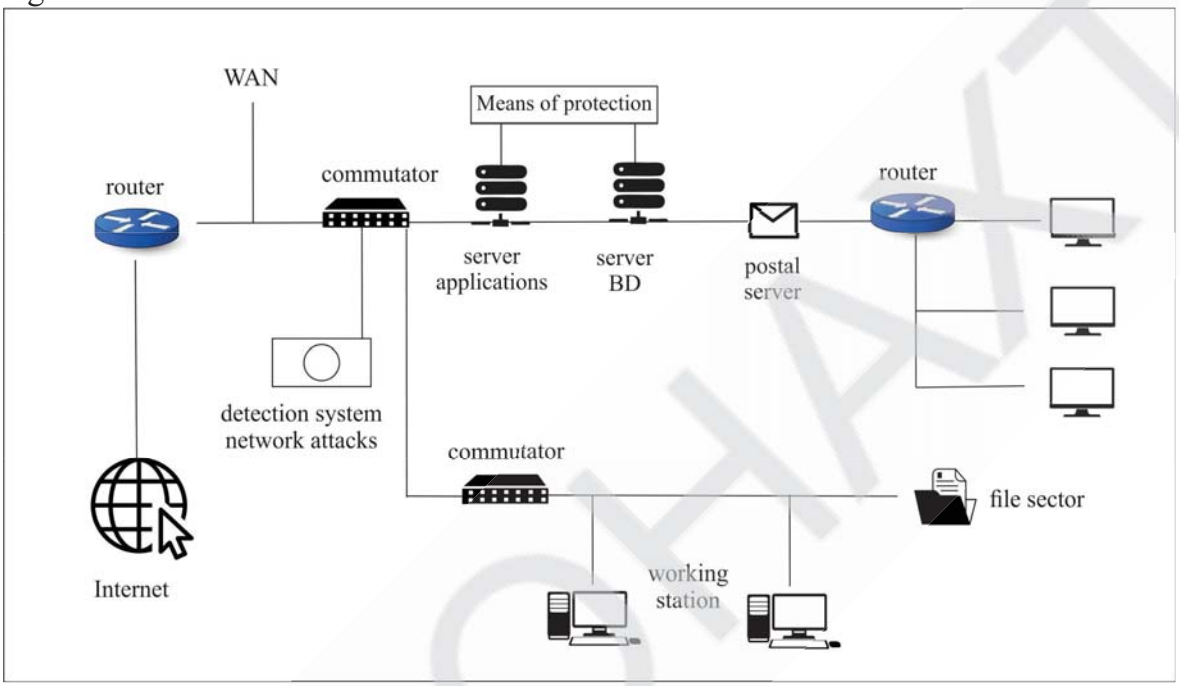

Рис. 2. Структурна схема підсистеми захисту інформації в СЕП

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

Table 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
	Via 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).

Table. 2. Protection of electronic payment systems

	EPS	Criteria															
		Protecting EPS accounts with password		Security when logging in to EPS	Automation with technical settings		Confirmation of a operations with 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	СЕП	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 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.

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".

4.3. 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% [4].

V. 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.

VI. LIST OF REFERENCES

1. Akhramovich, VM, Chegrenets, VM (2019). Information bank risk management of a commercial bank. Modern information protection. №2 (38), 54-59. http: // DOI: 10.31673 / 2409-7292.2019.025459

2. Б 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.

3. Kravchenko IS, Drozd, IV (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), 141-148.

4. Національний банк України.(3 листопада 2020).Беззаперечні тренди карткового ринку у 2020 році – розрахунки в Інтернеті та безконтактні платежі. https://bank.gov.ua/ua/news/all/bezzaperechni-trendi-kartkovogo-rinku-u-2020-rotsi--rozrahunki-v-interneti-ta-bezkontaktni-plateji.

USE OF K-NEAREST NEIGHBOUR METHOD IN ANALYSIS OF STUDENT DATA FROM SURVEYS

Authors: ***Ekaterina Konstantinova, Kamen Kalchev***
Advisor: ***Tsankov Tsvetoslav***
Konstantin Preslavsky University of Shumen (Bulgaria)

Abstract. *The purpose of the publication is to analyze the method K-Nearest neighbor and its application in intelligent analysis of student survey data. Examples are given based on student success and satisfaction.*

Keywords: *Educational Data Mining, EDM, K-Nearest neighbor.*

I. INTRODUCTION

Educational Data Mining (EDM) is a new scientific branch with applications in data acquisition education. EDM is "Applying Data Mining techniques to a specific set of data obtained from educational settings to address important educational issues" [5].

The search for dependencies and connections between the data and education will lead to forecasts, evaluation of the factors related to the candidate management method, students' success ratio, the quality of the learning process, and others [3].

The choice of the "K-Nearest neighbor" method in data analysis for students is dictated by the information of the top 10 algorithms for data extraction identified by the International Conference on Data Mining (ICDM) of the IEEE in December 2006, are C4.5 (Decision Tree), k-Means, SVM, Apriori, EM, PageRank, AdaBoost, kNN, Naive Bayes and CART [6].

II. K-NEAREST NEIGHBORS – KNN

The K-nearest neighbor algorithm is an object classification algorithm that calculates the distance between each pair of objects from the training set by using an appropriate function to measure the distance between the two points. The algorithm uses a majority vote of the k nearest neighbors of the object to classify it [1].

Function for measuring distance:

Euclidean

$$\rho(x_i, x_j) = \sqrt{\sum_{k=1}^{m} w_k} \qquad (1)$$

where:

$x_i = \left(x_i^{(1)}, x_i^{(2)}, \dots, x_i^{(m)}\right)$ – vector of m-features of the i-th object

$x_j = \left(x_j^{(1)}, x_j^{(2)}, \dots, x_j^{(m)}\right)$ – vector of m-features of the j-th object

Other known functions for measuring distance between two points are: L_p – metric, $L_\bullet$ – metric, L_1 – metric, Lance-Williams function.

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa National Academy of Food Technologies

The collection includes student works of the participants of the competition, which were not included in the number of prize-winners. The texts of the competitive works are published in the form in which they were submitted by the authors. The authors of the articles are responsible for the content and form of submission of the material.

Responsible for the issue: Sergii Kotlyk

Computer typesetting and layout: Oksana Sokolova

Odessa 2021