Economic Sciences

Экономические науки

UDC 33

Clients' Perceptions Towards IT Security of e-banking in Bosnia and Herzegovina

[1] Nedim Makarević
[2] Secim Hikmet

[1-2] Cyprus International University, Cyprus
[1] Doctor of Business Administration candidate
Senior Advisor at AIRNET Technologie
E-mail: nmakarevic@air-net.de
[2] Professor

Abstract. Main objective of this research is to examine clients' perceptions in Bosnia and Herzegovina towards IT security of e-banking, to diagnose problems and try to give proper solutions. Survey was prepared based on six variables and specific questions assigned to each variable. Response rate was good and 207 respondents were surveyed.Overall results suggested a slight agreement in general, and they indicated that when it comes to IT security of online banking, several factors including privacy, control and intangible features are highly important for clients of Bosnia and Herzegovina. Clients do not perceive tangible features as important as they actually are. Therefore, banks are those who need to give more effort when it comes to implementation of IT security in online banking. They definitely need to find more effective ways to inform and educate clients about IT security of using online service, and in that way create additional value.

Keywords: perceptions; IT security; online banking.

Introduction.

One of the ways to handle money with no physical contact and make money transactions is to use internet. This method resulted in whole new trend nowadays known as "online banking". According to Muniruddeen Lallmahamood (2007) internet banking refers to banking services over the public network (the Internet), through which customers can use different kinds of banking services ranging from the payment of bills to making investments. Internet banking or online banking has created new ways of handling banking transactions for banking related services and for e-commerce related transactions such as online shopping [1].

From mentioned information, it is easy to conclude that hackers can steal more money in their pajamas from their bed rooms than robber with a gun who is conducting robbery. Additionally, it is obvious that banks' dependence on new technologies increases, and therefore their need to protect their own and assets of their clients increases as well. This is where importance of IT security for banks' clients starts. Accordingly, it is important to know awareness level and perceptions of clients towards IT security of online banking. Since results of this research will enable banks to learn more about their clients, this research have potential to be important source of information to consider by banks when it comes to their planning and development activities. In Bosnia and Herzegovina (B&H), there is a need to do this research because there is a gap in literature about mentioned issue in this country. The latter fact gives even more value to this work.

When it comes to methodology of this work, survey based on specific variables has been prepared and distributed to clients who are actively using online banking.This research has objective to learn perceptions of clients when it comes to IT security of online banking in B&H. Main contribution of this research is consisted of providingnew information to banks operating in B&H andfilling the gap in literature when it comes to writing about this issue considering population of B&H as target.

Therefore, in the following sections of this work, through theoretical background, all necessary definitions together with brief historical facts important for understanding this topic will be explained. After that, information about online banking in B&H will be provided so readers can be more familiar with the situation in this country. Then, used methodology will be explained, after which results will be analyzed and discussed. In the end, appropriate conclusion will be prepared.

Theoretical background. Muniruddeen Lallmahamood (2007) defines internet banking as banking services over the public network (the Internet), through which customers can use different kinds of banking services ranging from the payment of bills to making investments [1]. On the other hand, Jagdeep Singh (2012) defines internet banking as online systems which allow customers to plug into a host of banking services from a personal computer by connecting with the bank's computer over the telephone wires. He is also mentioning some synonyms for internet banking such as online banking, PC banking, home banking or electronic banking [2].

According to Gordon and Loeb (2002), Information security is concerned with the protection of three characteristics of information: confidentiality, integrity, and availability through the use of technical solutions and managerial actions [3]. Banks are not only dealing with intangible money transactions, but also with protection of highly sensitive information such are credit cards' PINs, data about the customers, customers bank accounts and all other kinds of information that could enable to third party conducting the criminal activities and making damage for both, customer and bank. According to Landwehr (2001), weaknesses of banks' information systems are named vulnerabilities, and it is likely that such vulnerabilities represent opportunities for crime by third parties [4].

People were always trying to find appropriate way to protect their important and valuable assets. When considering different solutions for this problem throughout the history, it is interesting to mention that in Wild West, banks kept large amounts of cash, gold and silver on hand, and it was not difficult to trace them. Because of primitive communications and transportation, it might have been hours before the legal authorities were informed of a robbery and days before they could actually arrive at the scene of the crime, by which time the robbers were long gone. Since, guard for the night was only marginally effective, criminals needed only a little common sense and several days to analyze the situation. All mentioned factors tipped very much in the favor of the criminal. Today, highly sophisticated alarms and camera systems make asset protection easier. Also, banks stored money in safer forms, and many of them contain less cash than retail stores. The more cash it has, the more levels of security exist in particular bank. Additionally, because of communication and transportation improvements, police can be at the location in minutes. One of the alternatives when it comes to keeping money in safer forms than cash is electronic handling of money, where no physical contact is necessary. This means that almost all transactions can be realized via different devices including computers, mail or telephone, without physical contact. Such an operation resulted in new types of crime, and some of them are still new to the legal systems. Main problem is that allowing people to make transactions with no physical contact opens the door for criminals to gain access and make transactions. Accordingly, beside the physical security systems of banks, possibility of crime is still very high. Sometimes, in order to keep public image, banks do not even investigate and prosecute cybercrimes. If they would do that, customers wouldn't deposit money in their banks [5]. In short, big question emerge in heads of clients: "Is electronic way of handling money safe?"

Online banking in Bosnia and Herzegovina

According to report by Central bank of Bosnia and Herzegovina, only in 2007 more than 24 million of transactions were realized. Total value of mentioned transactions was 3,5 billion BAM. Average amount per transaction was 145 BAM. According to information from this report prepared at the end of 2007, at that point of time there were 31 commercial banks in B&H. Even 27 of them were using e-banking, which is 87,097 %. Still, few clients are using e-banking services. Number of clients who are making transactions through some way of electronic banking is only 10 692 individuals, and 5 308 legal entities. When we consider size of market of Bosnia and Herzegovina when it comes to banking services, this is relatively small number [6]. According to information above, there is a mismatch between supply and demand when it comes to e-banking services. Even though most of the banks offer e-banking services, still there are very few clients who are using them. Reason for this is still unknown. Therefore, this research will try to give an

answer from the aspect of IT security. In other words, IT security will be proven or eliminated as potential reason for non-acceptance of e-banking services by clients in Bosnia and Herzegovina.

Literature review.

Many researchers emphasized the risks that are emerging from adoption of new technologies by banks, and importance of IT security that increases along with new trends. Shrinath (1997) said that statement „information is power" hasnowhere been realized more significantly than in the banking industry. According to him, IT in banking normally refers to the core banking systems used for processing various kinds of commercial transactions in different products. When discussing the risks and challenges for IT security in that period of time, author mentioned four risks: unauthorized system/data access by business users in the bank; unauthorized system/data access by application/system support personnel; unauthorized system/data access by customers; unauthorized system/data access by the public at large. Since most people do not realize that large banks are prone to high risk of security breakdown even withoutgoing so far as the Internet, author decided to examine and explain the most critical areas[7].

Carl E. Landwehr (2001) states that in that period of time (which is 11 years ago) computers had shrunk so that a web server can be hidden in a matchbox and had become so common that few people could give an accurate count of the number they have in their homes and automobiles, much less the number they were using in the course of a day. Also, due to fact that computers constantly communicate with one another, the meaning and implications of "computer security" have changed over the years as well. Therefore, through his paper, Landwehr (2001) reviewed major concepts and principles of computer security [4].

Lawrence A. Gordon and Martin P. Loeb (2002) wrote an article which presents an economic model that determines the optimal amount to invest to protect a given set of information. Their model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. They show that for a given potential loss, a firm should not necessarily focus its investments on information sets with the highest vulnerability because vulnerable information sets may be inordinately expensive to protect. Therefore, it could be more useful for a company to focus on information sets with midrange vulnerabilities. After analysis conducted by Gordon and Loeb (2002), they suggested that in order to maximize the expected benefit from investment in information protection, a firm should spend only a small fraction of the expected loss due to a security breach [3].

Pikkarainen et al. (2004) conducted a study about consumer acceptance of online banking. They investigated online banking acceptance in the light of the traditional technology acceptance model (TAM). The data for their results was consisted of group interview with banking professionals, TAM literature and e-banking studies. According to their results, perceived usefulness and information on online banking on the Web site were the main factors influencing online-banking acceptance [8].

When it comes to explanation of basic concepts involved with system security, helpful was introductory chapter of book entitled „Security in computing "written by Charles P. Pfleeger& Shari Lawrence Pfleeger (2006). Their book deals with broad range of computer security related topics such are: cryptography; secure systems development; basic communications technologies; advices on planning, risk, and policies; Intellectual property; computer crime, and ethics. In short, it is possible to conclude that this book can serve as great guide to information about computer security attacks and countermeasures [5].

Luis V. Casalo, Carlos Flavian and Miguel Guinaliu (2007) made research with purpose to analyze the influence of perceived web site security and privacy, usability and reputation on consumer trust in the context of online banking. Their paper described the positive effects of security and privacy, usability and reputation on consumer trust in a web site in the online banking context. This study is very interesting and valuable since it proposes link between security, privacy and trust, amongst others, in the online banking context[9].

The study conducted by MuniruddeenLallmahamood (2007) explores the impact of perceived security and privacy on the intention to use Internet banking. Author used an extended version of the technology acceptance model (TAM) is to examine the above perception. Author concluded that while perceived usefulness is a critical factor in explaining users' intention to use Internet banking, it is important to pay attention to the security and privacy of users' of Internet banking. According to results, convenience, ease and time saving are the main reasons for the

adoption of Internet banking, whereas security, trust and privacy appear to be the top main concerns for non-Internet banking users. As author mentioned, this may also imply that security concerns and privacy protection are perceived to be part of the overall service provided by the Internet banking services providers, and he suggests that banks should gain customers' confidence through raising security levels of the bank [1].

IT security influence trust of clients as important factor. Best evidence for that is fact that most of articles that are dealing with evaluation of clients' trust when it comes to banking are including „security" as important construct. Accordingly, Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010) wrote a paper with aim to examine the role of situation normality cues (online attributes of the e-banking web site) and structural assurance cues (size and reputation of the bank, and quality of traditional service at the branch) in a consumer's evaluation of the trustworthiness of e-banking and subsequent adoption behavior. One of their findings in this work stated that web site features that give customers confidence are significant for promotion of e-banking [10].

Useful research for this article is also one completed by Mohanad Halaweh (2012) who was writing about user perceptions of e-commerce security[11]. In fact, both online banking and e-commerce are having common characteristic which is no physical (face to face) contact between parties involved in transaction, and using same technologies for doing transaction. This means that both of them are exposed to same risks. Accordingly, this common characteristic was very useful while identifying relevant variables for this study since some of them are simply modified and used for this research. Results of study conducted by Mohanad Halaweh (2012) showed that user characteristics, psychological state and intangible security features have a significant influence on e-commerce security perception. Additionally, in contrast, tangible security features and cooperative responsibility have a non-significant influence [11].

According to Singh (2012) customers, both corporate as well as retail ones are no longer willing to queue in banks, or wait on the phone, for the most basic of services. Therefore, electronic delivery of banking services is becoming the ideal way for banks to meet their clients' expectations. Accordingly, author got idea to study the scenario of e-banking, and in his study he considered opinions of 100 customers from Ludhiana. The results of this work revealed that people are aware of e-banking, but not fully. In fact, the Customers are at ease after using e-banking since it saves the precious time of the customer. It has also been found that Customer satisfaction varies according to age, gender, occupation etc. [2].

After going through literature review given above, it is obvious that there are strong interrelationships between privacy aspect, control aspect, psychological aspect, tangible features, intangible indicators on one side, and perceived IT security of e-banking on the other side. Therefore, it will be interesting to examine perceptions of Bosnian clients when it comes to mentioned factors regarding IT security of online banking.

Variables & survey

In order to get closer insight into clients' perceptions towards online banking in Bosnia and Herzegovina, six variables were identified as a result of literature review. Those variables are as follows:

1.1. Privacy aspect refers to confidence in the technology and online banking service provider when it comes to protection against privacy issues such are private information of client, information about money transactions conducted by client, information about client's personal passwords etc. Pikkarainen et al (2004) stated that as the amount of products and services offered via the Internet grows rapidly, consumers are more and more concerned about security and privacy issues [8].

1.2. Control aspect- When it comes to control perspective of IT security, as it is possible to conclude from survey questions of Yap, K. B., Wong, D. H., Loh, C., &Bak, R. (2010), this aspect refers to strictness of identity ascertaining when sending messages to client, or doing transactions by client, but also general control by bank when it comes to online transactions' confidentiality [10].

1.3. Psychological aspect- According to Halaweh, Mohanad (2012) The psychological aspect of security incorporates the feeling of fear, the need to feel that one's money is secure, and the ability to control the payment process and performance of online transactions. Even though he made research about e-commerce, because of same nature of e-commerce and e-banking which is

remote rather than face-to-face, his work was useful for preparation of survey in this study [11]. Therefore, it is possible to conclude that many customers have the misconception that the use of e-banking is vulnerable and that there is a high probability that their money will be lost.

1.4. Tangible features - Halaweh, Mohanada (2012) defines tangible indicators as those technological security features of websites that can be checked by users, such as https, padlocks and security certificates. Tangible features need to be understood and checked by the customer over the website rather than captured through social communication; this involves having knowledge and experience of these features, such as knowing what a security certificate means and how to check whether it has expired [11].

1.5. Intangible indicators - When talking about intangible indicators such are famous website and reputation, Halaweh, Mohanad (2012) says that they are not seen on the website and cannot be directly checked over the website. They are affected by society in terms of communication and the environment: where the customer lives and what they hear from others, as well as their past experience [11].

1.6. Perceived IT securityPerceived IT security refers to general perception of online e-banking services by clients when it comes to IT security.

Based on those variables, survey consisted of twenty questions was created. Questions were mainly adapted from previous researches considering Pikkarainen et al [8], Casaló, Flavián, and Guinalíu [9], Yap, K. B., Wong, D. H., Loh, C., & Bak, R. [10], Halaweh, Mohanad [11], Muniruddeen Lallmahamood [1]. In Table 1, questions prepared for the survey, together with their references they were adapted from are presented.

Table 1: Review of survey questions

Questions	Adapted from
I trust in the ability of bank to protect my privacy	Pikkarainen et al (2004)
I am not worried about my personal information given to bank	
I think that my bank's information system respects personal data protection laws	Casaló, Flavián, and Guinalíu (2007)
I think that my bank's information system will not provide my personal information to other companies without my consent	
I think that my bank's information system respects user's rights when obtaining personal information	
I think that bank needs to ascertains my identity before sending any messages to me	Yap, K. B., Wong, D. H., Loh, C., &Bak, R. (2010)
I think that bank needs to ascertains my identity before processing any transactions received from me	
I trust that my bank uses security controls for the confidentiality of online transactions	
I don't fear when I am using e-banking services	Halaweh, Mohanad (2012)
I never have misconceptions about using e-banking services	
I don't feel anxious to use e-banking services because of its nature, which involves a lack of face-to-face communication	
I feel safe when I release credit card information through Internet banking	Lallmahamood, Muniruddeen (2007)

I don't check the presences of http(s) in the URL when I handle money transactions online	Halaweh, Mohanad (2012)
I don't check the small padlock icon on the bottom right corner of the website when I handle transactions online	
I don't check the digital security certificate of the web site when I handle money transactions online	
I would use e-banking services only provided by on a reputable bank	Halaweh, Mohanad (2012)
I would use e-banking services only provided by local bank	
I think my bank shows great concern for the security of any online transactions	Casaló, Flavián, and Guinalíu (2007)
I believe using e-banking services online is secure	Halaweh, Mohanad (2012)
Using e-banking services gives me a feeling of security	

As already mentioned, Pikkarainen et al. (2004) conducted group interview with banking professionals in order to learn about consumer acceptance of online banking [8]. Specific questions related to privacy aspect from his interview were adapted and used in this research to examine clients' concerns about their privacy and security issues in e-banking.Casaló, Flavián, and Guinalíu (2007) made research with purpose to analyze the influence of perceived web site security and privacy, usability and reputation on consumer trust in the context of online banking [9]. Since they are dealing with similar issue, questions regarding security and privacy were adapted and used in this study. Yap, K. B., Wong, D. H., Loh, C., &Bak, R. (2010) used survey to evaluate trustworthiness of e-banking and subsequent adoption behavior through several factors [10]. Accordingly, several questions helpful to measure control aspect of IT security in e-banking were used in our study.Halaweh, Mohanad (2012) studied user perceptions of e-commerce security [11]. Since both e-commerce and e-banking are having the same characteristics such is lack of face to face communication and physical contact which implies same issues and concerns for final users of such a services, many questions were adapted from his survey in order to measure psychological aspect, tangible and intangible indicators, and perceived IT security in general when it comes to online banking. Also, when it comes to MuniruddeenLallmahamood (2007), one of questions used in his study was useful to adapt for this research when it comes to measuring psychological aspect of IT security [1].

Data and Methodology. Data for this study was collected by the means of a survey conducted in Bosnia and Herzegovina in 2013. A total of 250 questionnaire forms were delivered to respondents, and most of them were answered giving a response rate of 82.8percent.

Surveys were filled at universities by students, academic and administrative staff, and in branches of different commercial banks in Bosnia and Herzegovina by randomly selected clients. This resulted in a sample that was well distributed in terms of demographic information (e.g. age, and education).

Collected data is numerical except demographics part which is categorical. Seven point Likert scalewas used in order to test the agreements of the respondents on six variables through twenty questions. The collected data is then inserted into an excel spreadsheet and analyzed descriptively. The surveys were distributed both online and personally. Online version of survey was created, and its link was sent via e-mail to potential participants.

Results.

1.7. Demographics

Demographics information includes respondents' department, positions within the department and their education levels, gender and age. The survey is responded by 118 males and

89 females. Their education level is found to be extremely high (only twenty one respondents has no higher education level which is 10,1 % of all respondents). More details regarding education level of respondents are available in Table 2.

Table 2: Education level of respondents

Education level of Respondents	# of respondents	Percentage (%)
Other	21	10,1
Undergraduate	129	62,3
Master	53	25,6
Doctorate	4	1,9
Total	207	100

The positions of the respondents were grouped according to their similar characteristics. It is possible to conclude that most of respondents are still unemployed students, even 95 of them which is almost 46% of total number of surveyed respondents. Even though they are not employed, most of the students are studying far away from their hometown, and their parents (sponsors) are sending them money using banking services. This fact makes them considerable target for this research. When it comes to employed respondents, most of them are in managerial positions. Even 38 of surveyed people work in different managerial positions. Sample of 207 surveyed people has high level of variety in terms of positions, which is visible in Table 3.

Table 3: Positions of the Respondents

Positions of the respondents	# of respondents	Percentage (%)
Academic Staff	19	9,2
Accounting Officer	4	1,9
Administration	25	12,1
Electrical Engineer	1	0,5
Journalist	1	0,5
Lawyer	3	1,4
Librarian	2	1
Manager	38	18,4
Physical Worker	1	0,5
Psychologist	3	1,4
Sales Person	2	1
Software Developer	9	4,3
Teacher	2	1
Students (still unemployed)	95	45,9
Unemployed	2	1
Total	207	100%

1.8. Survey results

From Table 4, it is possible to conclude that privacy aspect of IT security in online banking of B&H is perceived as acceptable by clients of this region. In fact, mark of 5,223 indicates that clients slightly agree that bank is able, and doing its best to protect their privacy.

Table 4: Privacy aspect

PRIVACY ASPECT (5,223)	Mean	Std. Deviation
I trust in the ability of bank to protect my privacy	5,338	1,369
I am not worried about my personal information given to bank	5,188	1,487
I think that my bank's information system respects personal data protection laws	5,37	1,394
I think that my bank's information system will not provide my personal information to other companies without my consent	5,059	1,505
I think that my bank's information system respects user's rights when obtaining personal information	5,159	1,458

According to the results, clients think that high level of control is necessary when it comes to IT security of online banking. In other words, by selecting mark which is close to 6, clients confidentially agreed with statements about ascertaining their identities while using online banking and they believed that banks are using security controls to improve confidentiality of online transactions (Table 5).

Table 5: Control aspect

CONTROL ASPECT (5,594)	Mean	Std. Deviation
I think that bank needs to ascertains my identity before sending any messages to me	5,585	1,408
I think that bank needs to ascertains my identity before processing any transactions received from me	5,667	1,355
I trust that my bank uses security controls for the confidentiality of online transactions	5,532	1,457

When it comes to psychological aspect whose results are presented in Table 6, clients' perceptions towards IT security of online banking are shaky. In fact, respondents slightly agreed with the statements which indicate that still there is some space for fear, misconceptions and anxiousity while using online banking.

Table 6: Psychological aspect

PSYCHOLOGICAL ASPECT (5,221)	Mean	Std. Deviation
I don't fear when I am using e-banking services	5,322	1,529
I never have misconceptions about using e-banking services	5,345	1,482
I don't feel anxious to use e-banking services because of its nature, which involves a lack of face-to-face communication	5,285	1,655
I feel safe when I release credit card information through Internet banking	4,932	1,826

Results showed that users are not completely aware of importance of tangible features for security while doing online transactions. Clients in B&H were mainly neutral and slightly agreed that they are not very careful when it comes to paying attention to presence of http(s) in the URL, small padlock icon and digital security certificate of the web site. More details about this aspect are available in Table 7.

Table 7: Tangible Features

TANGIBLE FEATURES (4,563)	Mean	Std. Deviation
I don't check the presences of http(s) in the URL when I handle money transactions online	4,715	1,846
I don't check the small padlock icon on the bottom right corner of the website when I handle money transactions online	4,536	1,813
I don't check the digital security certificate of the web site when I handle money transactions online	4,439	1,78

On the other hand, this research showed that clients are paying more attention to intangible features such are banks' reputation, location and its concern towards security provision for its clients when making their decision to use online banking services. More details about influence of intangible features to clients' perceptions of IT security of online banking are available in Table 8.

Table 8: Intangible features

INTANGIBLE FEATURES (5,051)	Mean	Std. Deviation
I would use e-banking services only provided by on a reputable bank	4,955	1,673
I would use e-banking services only provided by local bank	5,048	1,579
I think my bank shows great concern for the security of any online transactions	5,15	1,649

When it comes to general opinion about IT security of online banking, from Table 9, it is possible to conclude that clients once again slightly agreed with the statements, and showed that they mainly agree that using e-banking services online is secure and that they mostly have feeling of security when using services of online banking.

Table 9: Perceived IT security

PERCEIVED IT SECURITY (5,208)	Mean	Std. Deviation
I believe using e-banking services online is secure	5,188	1,633
Using e-banking services gives me a feeling of security	5,227	1,592

Discussion of results.

The results suggested a moderate agreement in general except control aspect, which implies that clients perceive control as highly important when it comes to IT security. As it has been described by Casalo et al. [9], there are positive effects of security and privacy, usability and reputation on consumer trust in a web site in the online banking context. This research supported

mentioned statement, and it showed that IT security is definitely important factor for consideration by bank's clients. Also, Lallmahamod (2007) examined impact of perceived security and privacy on the intention to use Internet banking. Results indicated that security, trust and privacy appear to be the top main concerns for non-Internet banking users[1]. In this research, only users of online banking were surveyed, and according to results previously explained, it is possible to conclude that even though they use online banking, banks still didn't establish full trust with their clients. Even overall result of this research was moderate agreement, which doesn't have same level of confidentiality as strong agreement.Therefore, it would be interesting to make another research with non-users of online banking, and then compare their perceptions with perceptions of users in this research. Also, fact that users of online banking services are not completely aware of importance of tangible features for security while doing their transactions indicates that clients do not have enough knowledge about IT security of online banking. Therefore, banks in Bosnia and Herzegovina should find ways to inform and educate users about utilization of tangible features such are presence of http(s) in the URL, small padlock icon and digital security certificate of the web site in order to improve IT security of their services.

Conclusion.

This research proved to be in the aim to provide important insights in the area of clients' perceptionstowards IT security of online banking in Bosnia and Herzegovina. Also, the response rate of 82.8% together with the fact that surveyed people are coming from various companies, departments and positions within thosedepartments gives even more importance and value to the results of this work. Moreover, this work is not only diagnosing specific issues in terms of IT security of online banking in B&H, but also suggesting potential solutions. Main limitations of this research are relatively small sample and the generic approach to problem. Therefore, future researches can go more deeply into the issue and analyze larger samples. Because of the lack of available research about this issue in Bosnia, this is a very unique set of information for the banks operating in B&H. In the end, it is possible to conclude that when it comes to IT security of online banking, privacy, control and intangible featuresare highly important factors for clients of Bosnia and Herzegovina. On the other hand, clients do not perceive tangible features as important as they actually are. It is suggested for future research of similar type to focus on larger sample as mentioned previously, and to include non-users of online banking in research as well.

References:

1. Lallmahamod, M. (2007). An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce, 12*(3).

2. Singh, J. (2012). SCENARIO OF E-BANKING IN TODAY'S LIFE-A Survey. *International Journal of Computing & Business Research*.

3. Gordon, L., & Loeb, M. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457.

4. Landwehr, C. (2001). Computer security. *International Journal of Information Security*, *1*(1).

5. Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing* (4th ed.). Prentice Hall.

6. Public Relations Office of Central Bank of Bosnia and Herzegovina. (2007). *Information about cards management and electronic banking in Bosnia and Herzegovina.* Central Bank of Bosnia and Herzegovina, Public Relations Office, Sarajevo. Retrieved from http://www.cbbh.ba/pdf.php?id=539&lang=hr

7. Shrinath, B. (1997). Information Security in Banks. *Journal of Financial Crime, 5*(1), 65–71.

8. Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Research, 14*(3), 224–235.

9. Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review, 31*(5), 583–603.

10. Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010). Offline and online banking – where to draw the line when building trust in e-banking? *International Journal of Bank Marketing, 28*(1), 27–46.

11. Halaweh, M. (2012). Modeling user perceptions of e-commerce security using partial least square. *Journal of Information Technology Management, 23*(1).

УДК 33

Представления клиентов об информационной безопасности электронных банковских услуг в Боснии и Герцеговине

[1] Недим Макаревич
[2] Секим Нукмет

[1-2] Кипрский Международный Университет, Кипр
[1] Доктор делового администрирования
Старший советник технологии AIRNET
[2] Профессор

Аннотация. Главной задачей данного исследования является изучения представления клиентов Боснии и Герцеговины об информационной безопасности электронных банковских услуг, диагностирование проблем и попытки предложить правильные решения. Исследование было основано на шести переменных и специальных вопросах, составленных для каждой переменной. Процент ответивших был высоким, были опрошены 207 респондентов. Результаты продемонстрировали небольшое совпадение мнений и показали, что когда дело касается информационной безопасности электронных банковских услуг, несколько факторов, включая секретность, контроль и нематериальные характеристики очень важны для клиентов Боснии и Герцеговины. Клиенты не осознают насколько важны материальные характеристики. Таким образом, банкам необходимо прилагать больше усилий для внедрения информационной безопасности в электронные банковские услуги. Им определенно нужно находить более эффективные способы информирования и обучения клиентов об информационной безопасности использования электронных услуг и, таким образом, придавать им дополнительную ценность.

Ключевые слова: представления; информационная безопасность; электронные банковские услуги.