sciendo CzOTO 2019, volume 1, issue 1, pp. 112-119

# THE SECURITY OF INFORMATION CHANNELS IN BANKING SERVICES

doi: 10.2478/czoto-2019-0014
Date of submission of the article to the Editor: 30/11/2018
Date of acceptance of the article by the Editor: 28/01/2019

**Marcin Olkiewicz**[1]– *orcid id: 0000-0001-6181-6829*
**Mariusz Terebecki**[2] – *orcid id: 0000-0002-2455-2067*
**Radosław Wolniak**[3] – *orcid id:0000-0003-0317-9811*
[1]Koszalin University of Technology, Faculty of Economic Sciences, **Poland,**
*marcin.olkiewicz@tu.koszalin.pl*
[2]Pomeranian University in Słupsk, Faculty of Management and National Security, **Poland**
[3]Silesian University of Technology, Organization and Management Faculty, **Poland**

**Abstract:** This study focuses on the aspects related to the information technology security, and in particular, the quality of information security. It is inter alia because of international technology security that banks incur expenses to adapt their IT systems to guidelines of the supervisory authorities and to the expectations of international financial markets and stakeholders.
The constantly growing demands of stakeholders increasingly force the provision of services to be on the highest standard and delivered by means of new technologies. Therefore, banks adjusting their products and services to the requirements of stakeholders have to implement modern methods to secure information channels, thus guaranteeing information security to the stakeholders of a bank.
The aim of this paper is to present crucial security aspects in electronic banking, which indirectly affect the quality and security of the offered banking service and whether clients are aware of the most commonly occurring threat - an attack on a computer (phising). The source of data for this research was a group of 90 active users of information technologies, the analysis of certificates and securities used at the time of contact between the customer and the bank through an internet platform and a report of PRNews.pl on the state of banking in Poland for the fourth quarter of 2016.
**Keywords:** information, banking services, quality of security.

## 1.INTRODUCTION

The quality of customer service is one of the most important elements of creating a competitive advantage of a company, as well as part of responsible management (Wolniak, 2013; Wolniakand Skotnicka-Zasadzień, 2012). Banks, which are considered to be public trust institutions, pay attention to the quality of their services, especially in electronic banking, and above all to financial security(Alhothaily et al.,

2017; Wojciechowska-Filipek, 2015) of the recipients of information. The feeling of security by the bank's stakeholders indirectly influences, among others, the exchange of information about the bank and their products, adapted to society's quality of life (internet forums, social networks, etc.) as well as image and brand creation.
Electronic banking, as an innovation in the service delivery process, has become the current standard in banking, creating an added value for individual banks and their clients. This is due, in particular, to the rapid development of information technology at the end of the last century, which opened new information channels to the banking sector. It was thanks to the Internet that banks could switch away from telemarketing technology, which developed in the 1960s and to more advanced banking services provided remotely (remote banking). The lack of direct contact with the bank's employees makes it vital for the e-service to provide, process and generate all the necessary information which, through appropriate safeguards (Subsorn and Limwiriyakul, 2016; Alarifi et al., 2017), would create and guarantee a proper relationship between the bank and the client (Illia et al., 2015). While the issues related to the regulation of the financial market and payment services in Poland are strictly regulated by banking law (The Banking Act, 1997) and appropriate recommendations D and M (Recommendation D, 2013; Recommendation M, 2013) of the Polish Financial Supervision Authority (KNF, 2018), the use of online channels when sending commercial offers is an individual matter of particular banks (Rice and Sussan, 2016).

Difficulties in computerizing Polish banks result from constant changes in ownership as part of mergers or acquisitions, which is why the quality of the products offered, their assortment and availability are crucial elements of the banks' development. This is confirmed by the last three reports published by PRNews.pl at the end of March 2017, which summarize the fourth quarter of 2016 in the following areas: number of bank clients (PRNews.pl, 2016a), personal accounts market (PRNews.pl, 2016b) and online banking (PRNews.pl, 2016c). The presented data clearly indicate that the number of clients with access to electronic banking is gradually increasing and amounts to approximately 31 million. Constant changes in banking computer platforms are caused by modifications of IT solutions, resulting, among others, from potential security threats in basic system modules based on Internet channels. This trend may also result from the implementation of responsible bank management, as a part of management systems, through strategic activities focused on quality (Olkiewicz, 2004).

## 2. THEORETICAL BACKGROUND

Appropriate and responsible quality management, as part of continuous improvement, is the result of growing expectations and requirements of customers, as well as market risks visible, in particular, on the Internet. Fulfilling the needs and increasing the satisfaction of banking sector stakeholders requires high efficiency of the bank in the field of marketing - offering new products, as well as in information and communication technologies - guaranteeing a safe way of delivering and purchasing a service (Mujinga et al., 2018, Mann et al., 2015).
A modern IT banking system should be characterized by the following features (Ryznar, 2017; Chechen et al., 2016): focus on the customer, flexible design solutions, centralized nature of processing, comprehensive application and consistency of solutions, real-time data supply, services using modern technologies

such as data warehouses and data security.Therefore, it becomes purposeful to check the security measures implemented by individual banks for access to services from: the e-banking family, e.g. home/corporate banking, home/office-corporate banking, office-banking, corporate banking. Additionally, *Recommendation D* is adopted by the banks regarding information security management as preservation of confidentiality, integrity and availability of information, within the scope of data security included in the areas of accessibility, confidentiality, integrity, information settlement and non-compliance with current laws. Information protection activities in terms of strategic management of information technology and ICT environment security areas are in line with the ISO/IEC 27000:2009 management system. The analysis of risks occurring with threat scenarios causes the necessity to eliminate or minimize threats or their effects by securing banks under *Recommendation D*. *Recommendation D* contains 22 detailed guidelines in four "risk areas" of the ICT environment:

- strategy and organization of information technology and security areas
- development of IT environment,
- maintenance and operations in IT ,
- security management in IT.

From the point of view of this article, the Detailed Recommendation No. 16 of the abovementioned document is very important, the wording of which is as follows: "*Bank providing services with the use of electronic access channels should have effective technical and organizational solutions that ensure security of clients' identity, data and funds, and should educate clients on the principles of safe use of these channels*". It should be noted that pt.16.4. states that „*in addition, the bank should ensure that electronic banking connection sessions are encrypted and additional mechanisms are introduced that make these sessions resistant to the greatest extent possible to manipulations*".Additionally, pt. 16.8 highlights that „*the bank should inform clients about the risk related to in particular (…) other techniques designed to intercept information that allows access to the account (e.g. through attacks based on the phishing technique), together with an indication of the ways to protect oneself against such techniques*"(Recommendation D, 2013).

At this point, it is worth noting that in the process of appropriate quality management, pro-innovation activities (Olkiewicz, 2015) are undertaken that will allow the stakeholders to benefit from multi-channel banking. This means that currently the bank's stakeholders use various operating systems (Mann et al., 2015), which to a varying extent support the standards of modern Internet protocols aimed at securing the electronic communication channel between the client and the server. At the same time, they use different end devices (Lata, 2016) - they are not just PCs or laptops, but also tablets, smartphones, iPads, or mobile devices.Therefore, when using e-banking services in the communication process, certain messages are exchanged (i.e. communication standards), in which, among others, the protocol version, encryption and data compression methods are determined. Security certificates are also sent (unidirectional authentication and bidirectional authentication). which allow to check the identity of one of the parties or both sides.

Therefore, the services offered by the banks should be provided at the highest possible level, consistent with the current IT knowledge in the field of security and should be resistant to known types of attacks against the implemented security architecture. Internet attacks can be of various types, including*: phishing, cracking,*

*sniffing, snooping, back door, mole* etc. Therefore, online banking is secured by the computer operating systems, network management systems, data encryption techniques, and other bank security. The most commonly known security features include: *firewalls, certificates authenticating the connection with the bank (e.g. via RSA algorithm), data transmission security through message encryption (e.g. SSL protocol), password for private keys*, etc. It is worth noting that the security complexity providing a sense of security to the customer are the data processing levels indicated in the provided figures, which require complex calculations, e.g. using the critical encryption parameter, i.e. the key length. The longer the key, the harder it is to break, and thus decrypt the transmission.

## 3. RESULTS AND DISCUSION

Due to the complexity of the subject matter of the discussed area, the authors focused their attention in empirical research on the analysis of point 16 of *Recommendation D*, and in particular on:

1. *ensuring identity verification and data security;*
2. *assessment of clients' awareness regarding the rules of safe use of these channels*;
3. *client education.*

Research indicates that banking customers should, but not always do, pay attention to the presence of a "*green padlock*" on the browser toolbar, as it indicates a secured connection. In addition, all connections with e-banking services should be preceded by an internet address starting with *https://.* So what is behind the green padlock and the https protocol? By simply checking the security of a given website, the user can be ensured of the identity of the site and see for whom and by whom the security certificate was issued.

The conducted tests were based on reports generated by a special publicly available tool SSL Server Test. Detailed analysis showed (Terebecki and Olkiewicz, 2017) that the websites of the most popular banks are safe, which is confirmed by the data:

I. iPKO (https://www.pkobp.pl/); main data:

- Certificate used: RSA 2048 bits (SHA256withRSA).
- Supported protocols: TLS 1.2 (Yes); TLS 1.1 (Yes); TLS 1.0 (Yes); SSL 3 (No), SSL 2 (No)
- Encryption algorithms for TLS 1.2:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_3DES_EDE_CBC_SHA.

2. Inteligo (https://inteligo.pl/secure), main data:

- Certificate used: RSA 2048 bits (SHA256withRSA).
- Supported protocols: TLS 1.2 (Yes); TLS 1.1 (Yes); TLS 1.0 (Yes); SSL 3 (No), SSL 2 (No)
- Encryption algorithms for TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_3DES_EDE_CBC_SHA.

3. Pekao24 (https://www.pekao24.pl/), main data:

- Certificate used: RSA 2048 bits (SHA256withRSA).
- Supported protocols: TLS 1.2 (Yes); TLS 1.1 (Yes); TLS 1.0 (Yes); SSL 3 (No), SSL 2 (No)
- Encryption algorithms for TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA.

4. mbank (https://online.mbank.pl/), main data:

- Certificate used: RSA 2048 bits (SHA256withRSA).
- Supported protocols: TLS 1.2 (Yes); TLS 1.1 (Yes); TLS 1.0 (Yes); SSL 3 (No), SSL 2 (No)
- Encryption algorithms for TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA.
- Connection simulation failed:IE 6 / XP, IE 8 / XP.

5. Orange Finanse (https://orangefinanse.com.pl/), main data:

- Certificate used: RSA 2048 bits (SHA256withRSA).
- Supported protocols: TLS 1.2 (Yes); TLS 1.1 (Yes); TLS 1.0 (Yes); SSL 3 (No), SSL 2 (No)
- Encryption algorithms for TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA.

6. BZWBK24 (https://www.centrum24.pl/), main data:

- Certificate used: RSA 2048 bits (SHA256withRSA).
- Supported protocols: TLS 1.2 (Yes); TLS 1.1 (Yes); TLS 1.0 (Yes); SSL 3 (No), SSL 2 (No)
- Encryption algorithms for TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.

7. Moje ING (https://login.ingbank.pl/), main data:

- Certificate used: RSA 2048 bits (SHA256withRSA).
- Supported protocols: TLS 1.2 (Yes); TLS 1.1 (Yes); TLS 1.0 (Yes); SSL 3 (No), SSL 2 (No)
- Encryption algorithms for TLS 1.2:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.
- Connection simulation failed:IE 6 / XP.

The authors tried to emphasize that in the era of universal access to information and independent services, verification of bank connection security is not a major problem. It is worth noting that communication security is also ensured by other banks:

- Alior Bank (https://aliorbank.pl/hades/) – overall rating A;
- Bank BGŻ BNP Paribas iBGŻOptima (https://login.bgzbnpparibas.pl/) – overall rating A;
- Credit Agricole Bank Polska (https://e-bank.credit-agricole.pl/) – overall rating C;
- Bank Millennium (https://www.bankmillennium.pl/) – overall rating A+;
- Getin Noble Bank (https://secure.getinbank.pl) – overall rating A+;

- Eurobank (https://online.eurobank.pl/) – overall rating A+ with a prospect of lowering the rating to C;
- Bank Pocztowy (https://www.pocztowy24.pl/) – overall rating A;
- RaiffeisenPolbank (https://moj.raiffeisenpolbank.com/) – overall rating A;
- Citi Handlowy (https://www.online.citibank.pl/) – overall rating A;
- T-Mobile Usługi Bankowe (https://online.t-mobilebankowe.pl/) – overall rating A;
- Deutsche Bank (https://dbeasynet.deutschebank.pl/) – overall rating A;
- Plus Bank (https://plusbank24.pl/) – overall rating A;
- BOŚ (https://bosbank24.pl/) – overall rating A;
- Santander Consumer Bank (https://online.santanderconsumer.pl/) – overall rating A+ with a prospect of lowering the rating to C.

It is important that in the era of professional security in terms of implementing the appropriate level of encryption in internet banking, banks do not limit themselves only to securing information and marketing activities but they also offer them to the already existing portfolio of clients as well as potential future clients.

However, it should be remembered that security is best preserved with a high level of awareness regarding the principles of safe use of information channels. Lack of awareness of the risks and the unambiguous identification of electronic mailboxes may lead to a situation in which the bank client becomes a victim of phishing. This means that the bank's customer, the user of electronic mailbox, may not be able to distinguish an original message received from the bank from a false message. Already in 2014, the Polish Financial Supervision Authority issued a guide for clients of financial services titled "Financial security in electronic banking - financial crimes related to electronic banking", drawing attention to the possibility of such an attack. The guide is addressed to ordinary users and, as its authors indicate, its main goal is "... *raising the awareness of financial market participants in the area of threats related to the use of electronic banking, and disseminating the knowledge about the rules of conduct, compliance with which will largely protect them, as well as familiarizing with the issues related to the nature and specificity of crimes related to electronic banking* ... "(KNF, 2005).

In order to verify the level of awareness regarding the safety of using banks' information channels, the authors conducted a survey on a group of 90 active users (60 women, 30 men) of information technology. The surveyed group was appropriately profiled to include people who use the Internet on a daily basis. What is important, the studied population is mostly young (16.7% (aged 18-22), 64.4% (aged 23-27), 8.9% (28-32), and 10% (over 32 years)), who, due to their age, should belong to the conscious Internet users.

Studies have shown that 57.8% of all respondents did not know the concept of phishing, which means that there is lack of awareness of the existence of this most popular threat, which is also one of the simplest forms of computer attack. What's more, a phishing attack is quite often an introduction and preparation for a proper attack. Such an unconscious user, by clicking or downloading an unverified attachment, opens their computer for subsequent attacks.

However, in terms of issues related to the secure connection between the bank's customer and the server when online banking is used, as many as 75.6% of respondents draw attention to the so-called "green padlock", which means that up to 24.4% do not control security. Such a high rate of people who are unaware of threats

in communication channels or do not visually check the security of the Internet connection makes the level of computer attack threat high.The authors' satisfaction with the high level of security awareness of the respondents, resulting from controlling security by means of the so-called "green padlock" has been minimized by the fact that only 37.8% of the respondents make the effort to verify the safety certificate, which means that as many as 62.2% of people do not care about whom the certificate belongs to at the time of connection. And it should be remembered that connection verification is a verification of the security certificate, whether it's authentic and up to date. It can therefore be concluded that the society trusts electronic banking and is not always aware of the existing threats in communication channels.

## 4. CONCLUSION

The changing environment and uncertainty due to a very high level of complexity of the banking system forces the banks to undertake strategic activities in the area of broadly understood security. One of the areas of continuous improvement in the quality of information security is the search for and implementation of new methods and tools which, by increasing the efficiency of electronic banking activities, will minimize risks and their consequences. On the one hand, the analysis of reports confirms that all banks use strong encryption based on 2048-bit key. This encryption is based on RSA asymmetric encryption, and additionally, the banks support a secure TLS family protocol, while excluding the out-of-date SSL protocols. It is important that the supported protocols have all the recommended encryption algorithms. On the other hand, the survey indicates that bank customers have low awareness of the need to verify the security of transmission and the tools used to confirm the security of online banking services.

Summing up, the double-track study has shown the need for further more detailed studies that will accurately determine "blank spots" in the awareness of banking services users.

## REFERENCES

Alarifi, A., Alsaleh, M., Alomar N., 2017. *A model for evaluating the security and usability of e-banking platforms*. Computing, 99, 519–535, DOI 10.1007/s00607-017-0546-9.

Alhothaily, A., Alrawais, A., Song, T., Lin, B., Cheng, X., 2017. *Quick Cash: Secure Transfer Payment Systems.* Sensors, 1376(17); 1-20, doi:10.3390/s17061376

Chechen, L., Yi-Jen, H., Tung-Heng, H., 2016. *Factors influencing internet banking adoption.* Social Behavior and Personality, 44(9), 1443–1456, http://dx.doi.org/10.2224/sbp.2016.44.9.1443

Illia, A., Ngniatedema, T., Huang Z., 2015. *A conceptual model for mobile banking doption* Journal of Management Information and Decision Sciences, 18(1), 111-122.

KNF, 2018. https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/rekomendacje_dla_bankow?articleId=8522&p_id=18 (acccesed: 20.06. 2018)

Lata, P., 2016. *Role of Information Technology in Banking Sector.* Journal of Commerce & Management Thought, 7(1), 186-195, DOI: 10.5958/0976-478X.2016.00013.6

Mann, D., Travis, C.L., Lloyd Cook, D., 2015. *Data Security and Privacy: More than the IT Department's Concern.* The Computer & Internet Lawyer*,* 32(12), 8-11.

Mujinga, M., Eloff, M.M., Kroeze, J.H., 2018. *System usability scale evaluation of online banking services: A South African study.* South African Journal of Science, 114(3/4), 16-19.

Olkiewicz, M., 2015. *Knowledge management as a determinant of innovation in enterprises.* Proceedings of the 9th International Management Conference "Management and Innovation For Competitive Advantage", Bucharest, Romania, 399-409.

Olkiewicz, M., *Zarządzanie jakością w sektorze bankowym w dobie wejścia do Unii Europejskiej.* Rynki finansowe w przestrzeni elektronicznej, (ed.) B. Świecka, Wyd. Uniwersytet Szczeciński, Szczecin 2004, 183-191.

PRNews, 2016(a). *Report: Number of bank clients – IV quarter of 2016*. http://prnews.pl/wiadomosci/raport-prnewspl-liczba-klientow-w-bankach-iv-kw-2016-6554091.html (accessed: 31.03.2017r.)

PRNews, 2016(b). *Report: Personal accounts market – IV quarter of 2016*. http://prnews.pl/raporty/raport-prnewspl-rynek-kont-osobistych-iv-kw-2016-6553975.html (accessed: 31.03.2017r.)

PRNews, 2016(c). *Report: Internet banking market – IV quarter of 2016*. http://prnews.pl/wiadomosc/raport-prnewspl-rynek-bankowosci-internetowej-iv-kw-2016-6554056.html (accessed: 31.03.2017r.)

Recommendation D, 2013. https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf (accessed: 20.06.2018).

Recommendation M, 2013. https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_M_8_01_2013_uchwala_8_33017.pdf (acccesed: 20.06.2018)

Rice, J.C., Sussan, F., 2016. *Digital privacy: A conceptual framework for business*. Journal of Payments Strategy & Systems, 10(3), 260-266.

Ryznar, Z., 2017.*Zarys historii komputeryzacji banków w Polsce*. Polska informatyka: systemy i zastosowania, (ed.) J.S. Nowak, B. Ostrowska, Wyd. Polskie Towarzystwo Informatyczne, Warszawa, p.184.

Subsorn, P. Limwiriyakul, S., 2016. *An Investigation of Internet Banking Security of Selected Licensed Banks in Vietnam*. Walailak J Sci & Tech; 13(6), 411-432.

Terebecki, M., Olkiewicz, M., 2017. *Jakość zabezpieczeń informacji determinantą rozwoju bankowości internetowej.* Studia nad bezpieczeństwem, 2, 143–162.

*The Banking Act of 29 August 1997*. Journal of Laws. 1997 no 140 pos. 939.

Wojciechowska-Filipek, S., 2015. *Zarządzanie jakością informacji w organizacjach zhierarchizowanych*. CeDeWu, Warszawa, Polska.

Wolniak, R., 2013. *The assessment of significance of benefits gained from the improvement of quality management systems in Polish organizations.* Quality & Quantity, 47(1), 515-528, DOI:10.1007/s11135-011-9534-x

Wolniak, R., Skotnicka-Zasadzień B., 2012. *The concept of study of Servqual method's gaps*. Quality & Quantity, 46(4), 1239-1247. DOI 10.1007/s11135-011-9434-0.