THREATS TO THE SECURITY OF INFORMATION MANAGEMENT IN THE FIELD OF ELECTRONIC BANKING

ZAGROŻENIA DLA BEZPIECZEŃSTWA ZARZĄDZANIA INFORMACJAMI W DZIEDZINIE BANKOWOŚCI ELEKTRONICZNEJ

Marzena Hajduk-Stelmachowicz[1]

RZESZÓW UNIVERSITY OF TECHNOLOGY

Karolina Iwan[2]

RZESZÓW UNIVERSITY OF TECHNOLOGY

Abstract: Digitisation and, the closely related thereto, technological progress have also found their way into the cybercrime aspect. Particularly vulnerable to this phenomenon are institutions that handle confidential information – especially financial institutions. The main purpose of the paper is to present a typology of threats having an impact on the way of managing information by the users of electronic banking. The paper points out the need to understand the essence of information management security. It emphasises the importance of taking regular actions, not only in the organisational perspective, but also in the individual perspective. The results of secondary research, as analysed in the paper, allow to outline the scale of the cybercrime problem in electronic banking. Besides, they show a disturbingly low level of awareness among ordinary people as regards the application of security measures to increase the level of safety in the usage of financial services by individuals.

Streszczenie: Digitalizacja i ściśle z nią związany postęp technologiczny również znalazły swoje miejsce w aspekcie cyberprzestępczości. Szczególnie narażone na to zjawisko są instytucje, które zajmują się informacjami poufnymi – zwłaszcza instytucje finansowe. Głównym celem artykułu jest przedstawienie typologii zagrożeń mających wpływ na sposób zarządzania informacjami przez użytkowników bankowości elektronicznej. W artykule zwrócono uwagę na potrzebę zrozumienia istoty bezpieczeństwa zarządzania informacjami. Podkreśla się znaczenie podejmowania regularnych działań, nie tylko w perspektywie organizacyjnej, ale również w perspektywie indywidualnej. Wyniki badań

[1] Rzeszów University of Technology, Faculty of Management; e-mail: marzena.hajduk@ur.edu.pl.

[2] Rzeszów University of Technology, Student Scientific Circle of Young Economists; e-mail: karolina.iwan@ur.edu.pl.

wtórnych, przeanalizowane w artykule, pozwalają na zarysowanie skali problemu cyberprzestępczości w bankowości elektronicznej. Ponadto wykazują niepokojąco niski poziom świadomości zwykłych ludzi w zakresie stosowania środków bezpieczeństwa w celu zwiększenia poziomu bezpieczeństwa korzystania z usług finansowych przez osoby fizyczne.

Keywords: electronic banking, information security management, cyberattacks, cybercrime.

Słowa kluczowe: bankowość elektroniczna, zarządzanie bezpieczeństwem informacji, cyberataki, cyberprzestępczość.

Introduction

The cybercrime incidents presented in the media[3] that take place in almost every corner of the world have been more and more alarming[4].

According to the Wyborcza.pl portal, the most serious cyberattack in history took place in May 2017. "The list of victims (…) of cybercriminals includes, among others, the Russian government, courier company FedEx, hospitals in Great Britain, Indonesia and South Korea, and Chinese schools". In total, the cyberattacks were carried out in as many as 99 countries. Among the victims of the attack was, *inter alia*, a Russian mobile phone operator and some banks[5]. The attack was carried out with the use of ransomware[6]. After infecting the computers, a ransom of 300 dollars was demanded. Varum Badwhar, security expert, admitted that it had been the first time that it had taken only a day to spread the attack[7].

In 2016, the staff of CERT Polska was involved in combating 1,926 cyberthreat incidents[8]. Compared to 2015, it is an increase by 32 percent[9]. The authors

[3] Cybercrime is a type of prohibited act committed in cyberspace. Cf. Ministry of the Interior and Administration, Rządowy Program Ochrony przed Cyberprzestępczością RP na lata 2011-2016 (The Government Program for the Protection of Cyberspace of the Republic of Poland for the years 2011-2016), Warszawa 2010.

[4] J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne" 2014, Vol. 1-2, p. 25.

[5] M. Bednarek, J. Wątor, *Rządy, firmy, szpitale i szkoły na celowniku hakerów. „Największy cyberatak w historii",* Wyborcza.pl 13.05.2017, http://wyborcza.pl/7,75399,21806893,rzady-firmy-szpitale-i-szkoly-na-celowniku-hakerow-najwiekszy.html (dostęp: 19.05.2017).

[6] Malicious software which encrypts data and blocks access to them.

[7] M. Bednarek, J. Wątor, *Rządy, firmy, szpitale i szkoły na celowniku hakerów. „Największy cyberatak w historii",* Wyborcza.pl 13.05.2017, http://wyborcza.pl/7,75399,21806893,rzady-firmy-szpitale-i-szkoly-na-celowniku-hakerow-najwiekszy.html (dostęp: 12.07.2017).

[8] Incidents can be reported through the website of CERT Polska https://www.cert.pl/zglos-incydent/

[9] *CERT: In 2016, cybercriminals mostly tried to fraudulently obtain information,* http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1036280,cyberprzestepcy-najczesciej-probowali-wyludzic-informacje.html (read on: 12 July 2017).

of the report pointed out that "the criminals use a wide range of solutions, in particular when they steal savings with the use of mobile devices"[10].

Criminals always carry out their hacker attacks in a carefully thought-out manner. Particularly vulnerable to the attacks of cybercriminals are financial institutions and their customers. Such institutions handle enormous amounts of valuable information[11]. Besides, they can be helpful in the context of using their resources for financial speculation[12]. Such institutions include for example banks that make use of electronic banking which is strictly associated with cyberspace[13]. The surveys "Perception of the Internet and new technologies in Poland" (conducted by the Orange Foundation (Fundacja Orange)), among the three spheres of life most affected by the Internet and development of new technologies (over the last 10 years) have indicated[14] the handling of financial matters, e.g. servicing a bank account (44% of responses). This is understandable because electronic banking ensures convenient transactions through easy access to cash (and thus saves us a trip to the bank)[15]. Thanks to the dynamics of development, it offers newer and more convenient solutions, both to the customers and the bank itself.

In the course of development and in-depth analysis of the cyberattack concept, it is worthwhile to point out the threats associated with the field of e-banking. The main purpose of this paper is to present examples of threats on the part of cybercriminals which can affect the users of electronic banking. The paper points out the need to manage information, which is treated as the importance of taking regular actions (integrating a number of interdisciplinary issues and problems of contemporary

---

10 Ibidem.

11 Cf. *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, P. Bogdalski, Z. Nowakowski, T. Płus, J. Rajchel, K. Rajchel (ed.), the Police Academy in Szczytno (WSP w Szczytnie), Warszawa 2013.

12 Cf. Z. Ciekanowski, J. Nowicka, H. Wyrębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Siedlce University of Natural Science and Humanities (Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach), Siedlce 2016.

13 The term cyberspace is to be understood as the digital space of processing and exchange of information created by ICT systems and networks together with links between them and the relations with users. Cf. Ministry of the Interior and Administration, Rządowy Program Ochrony przed Cyberprzestępczością RP na lata 2011-2016 (The Government Program for the Protection of Cyberspace of the Republic of Poland for the years 2011-2016), Warszawa 2010.

14 The Orange Foundation (Fundacja Orange), *Postrzeganie Internetu i nowych technologii w Polsce (Perception of the Internet and new technologies in Poland)*, Warszawa, Raport 2015 (2015 Report), p. 10, http://www.krrit.gov.pl/drogowskaz-medialny/aktualnosci/news,2123,postrzeganie-internetu-i-nowoczesnych-technologii-w-polsce.html (read on: 12 July 2017).

15 E. Hajduk, M. Hajduk, *Wybrane aspekty związane z wykorzystaniem Internetu w biznesie*, [in:] *Komputer – przyjaciel czy wróg?*, A. Szewczyk (ed), The University of Szczecin (Uniwersytet Szczeciński), Faculty of Economics and Management, Institute of Computer Science in Management, Printshop Publishing House, Szczecin 2005, pp. 367-373.

information science[16]), in the organisational and individual perspective. Such approach should be particularly emphasised (as is demonstrated by analysis of the literature on the subject)[17]. The method used in order to accomplish the purpose of the paper includes analysis of the selected literature on the subject.

1. Typology of crimes in the field of electronic banking

Along with technological progress, the number of crimes, which are becoming more and more difficult to control, even by the highest state authorities, has been constantly increasing[18]. The threat consisting in deliberate disruption of the proper functioning of cyberspace (without engaging the personnel or other users) that makes it possible to omit or weaken the hardware and software access control mechanisms[19], in a special way applies to the electronic banking services. Cyberattacks can occur both on the server and customer side (Fig. no. 1).

As stated in the report entitled "The security landscape of the Polish Internet in 2016", the CERT Polska[20] group was notified of over 722 thousand phishing incidents. According to Interia Biznes, "pretending to represent a financial institution, a telecommunications operator, a bank or a telecommunications company in order to fraudulently obtain data, usernames and passwords to bank accounts, i.e., phishing, was one of the biggest security threats of 2016. The current year is likely to be a record-breaking year in terms of phishing"[21]. Using deception in order to obtain personal information[22] consists in sending a message with a website address by criminals who disguise themselves as e.g. a financial institution[23]. The website address, sent by cybercriminals, to a large extent resembles access to the original bank site[24].

---

16 B. Sosińska-Kalata, *Obszary badań współczesnej informatologii (nauki o informacji)*, [in:] „ZIN – Issues in Information Science. Information Studies" („ZIN Studia Informacyjne") 2013, Vol. 2 (102), pp. 28-32.

17 *Nauka o informacji*, (ed.) W. Babik, the Polish Librarians' Association (SBP) Publishing House, Warszawa 2016, p. 368.

18 According to Control Risks, approx. 33% of cyberattacks in 2016 were against the public sector.

19 Cf. Ministry of the Interior and Administration, The Government Program... (Rządowy Program...), op. cit.

20 CERT Polska (Computer Emergency Response Team) is a team established in order to respond to incidents that violate online security of users or institutions. It has been operating since 1996 within the structure of NASK (the Research and Academic Computer Network).

21 Interia Biznes, *Phishing czyli rekordowe wielkie wyłudzenie*, http://biznes.interia.pl/raport/bezpiecznie-w-sieci/news/phishing-czyli-rekordowo-wielkie-wyludzanie,2489719,8636 (read on: 30 May 2017).

22 M. Capiga, *Bezpieczeństwo transakcji finansowych w Polsce*, op. cit., p. 179.

23 S. Wojciechowska-Filipek, *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010, p. 77 et seq.

24 D. Wawrzyniak, *Bezpieczeństwo bankowości elektronicznej*, [in:] „Bankowość elektroniczna", Gospodarowicz A. (ed.), Polish Economic Publishing House (PWE), Warszawa 2005, p. 72 et seq.

Table 1. Examples of threats occurring in the field of electronic banking

Threat sources common for the server and the customer Rely on eavesdropping and modification of data sent over the network	• **sniffing** – eavesdropping • **spoofing** – pretending to be a different computer in the network • **network snooping** – preliminary identification of network parameters, primarily with regard to security • **vishing** – criminals disguise as a bank in order to fraudulently obtain the customer's PIN and user ID to electronic banking • **phishing** – using fraudulent methods to obtain confidential personal information • **man-in-the-middle attacks** – a type of phishing, where criminals communicate via a fake website • **man-in-the-browser attacks** – an attack on the browser • **computer sabotage and cyberterrorism** • **threats to SMTP, MIME, POP,** etc. **services** • **DNS threats,** which mainly take advantage of service vulnerability to denial-of-service attacks
Customer related threats Associated with the procedures of logging in to the system and using customer software	• a threat of compromising system access parameters, such as ID or password • software and hardware manipulations aimed at changing their functionalities in a manner invisible to the user • standard software errors, e.g. online browser errors • non-standard software errors • viruses – harmful computer programs with the ability to replicate themselves
Server threats Including attacks on server resources	• DoS and DDoS attacks. It consists in attacking the computer system or network service in order to make it inoperable by occupying all the available resources (carried out simultaneously with the use of one or more computers), • attacks with the use of special programs (e.g. viruses, Trojan horses, logic bombs), which make it possible to interfere with the IT systems or databases, • threats caused by misfortunes and environmental incidents (e.g. fires, thunderstorms, floods), • threats caused by carelessness, errors, negligence, disloyalty and dishonesty on the part of the personnel.

Source: own work based on: M. Capiga, *Bezpieczeństwo transakcji finansowych w Polsce*, CeDeWu, Warszawa 2015, p. 179, [after:] S. Wojciechowska-Filipek, *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010, p. 77 et seq, D. Wawrzyniak, *Bezpieczeństwo bankowości elektronicznej*, [in:] *Bankowość elektroniczna,* A. Gospodarowicz (ed.), Polish Economic Publishing House (PWE), Warszawa 2005, p. 72 et seq.

Criminals induce users to go to a fake site by notifying them of the need to click on the link attached to the email. The need to take action is justified, among other things, by extending the validity of the card, its activation or improving the safety of its use. When an imprudent customer provides the required data, the criminals are given an opportunity to make transfers to the accounts that they have opened[25].

[25] *Bezpieczeństwo finansowe w bankowości elektronicznej…* op.cit., p. 40.

Cybercriminals are so professional that sometimes it takes quite a lot of time to notice the difference in a domain address[26]. An important aspect in the context of improving the security of online transactions is making sure that a given website has an encrypted connection to the server (the address should begin with "https", and next to it there should be the padlock icon)[27].

Another example of crime in the field of electronic banking is so called **skimming**. It involves the copying of information from the magnetic stripe of a payment card[28]. There are two types of skimming[29]:

- ATM skimming – involves making modifications to the ATM structure in order to copy the data and create a duplicate card,
- skimming at POS devices – involves the intercepting of data while the card owner is making a transaction.

The basic activity in case of ATM skimming is installation in the ATM of a device (skimmer) that scans payment card data. Such devices allow for both transmitting the intercepted data via radio waves to the criminal's computer and memorising them directly on the inserted memory card. The most important thing from the criminal's point of view is to scan the magnetic stripe of the payment card. "The magnetic stripe of an original payment card is divided into three tracks: the first one contains, stored in an open form, the first and last name of the cardholder, checksum, information relating to the country and bank issuing the card, the second one contains the card number, validity date and the service code for proper reading, while the third track is practically unused"[30]. Another important stage of an attack is the installation of a tiny camera and placing a fake keypad over the top of the genuine keypad on an ATM which then memorises individual PIN digits and stores them in the correct order on the reader. After obtaining all the necessary information, criminals are able to manage the card and the funds that it provides access to. In case of skimming at POS devices, the data from the card are e.g. scanned by a shop assistant who cooperates with the hackers or is a hacker himself. Copying the magnetic stripe is not too difficult, one only needs to approximate the card to a small scanning device. Then, the intercepted data from the magnetic stripe are transferred onto a "clean magnetic card" or onto an original payment card (often the stolen one).

---

[26] Cf. *Wyzwania informatyki bankowej*, A. Kawiński, A. Sieradz (ed.), The Gdańsk Institute for Market Economics (Instytut Badań nad Gospodarką Rynkową), – The Gdańsk School of Banking (Gdańska Akademia Bankowa), Gdańsk 2016.

[27] Strefa Biznesu, *Bankowość elektroniczna. Jak nie dać się okraść cyberprzestępcom*, http://www.pomorska.pl/strefa-biznesu/wiadomosci/z-kraju-i-ze-swiata/a/bankowosc-elektroniczna-jak-nie-dac-sie-okrasc-cyberprzestepcom,11409221/ (read on: 30 May 2017).

[28] M. Capiga, op.cit., p. 179.

[29] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, "Przegląd Bezpieczeństwa Wewnętrznego", Vol. 10/14, pp. 108-111.

[30] Ibidem, p. 110.

One more activity commonly used to carry out the attacks is spoofing. Criminals take control of a computer of another user and then use it for illicit activity[31]. Attacks based on **vishing** are growing in popularity. In this case fraudsters pretend to represent a bank and e.g. try to fraudulently obtain a username or password during a phone conversation. An attack based on vishing was used in 2015 by gang members operating in Great Britain. They telephoned randomly selected victims pretending to be police officers and asking for a card in connection with an investigation into alleged hacking into bank accounts. "When the victim consented, 'police couriers' knocked on their door to collect the card"[32]. The cards taken over from their holders were immediately emptied out.

The attacks that take place are nearly always based on malicious software, which includes popular computer viruses, logic bombs, computer worms and Trojan horses, so called Trojans. A computer virus is a type of program that becomes part of another program and has the ability to replicate. It can, among other things, delete data, steal data or even stop computer from working[33]. A computer worm has a similar effect, however "unlike a computer virus, it does not destroy data or transform files, but can put burden on computer programs (...) causing significant difficulties or even making it impossible to use them"[34].

An important and long-unnoticed threat are so called logic bombs which can "remain dormant for a long time and are activated at a specific date or at the moment when the user performs a specific action"[35].

The 2017 IBM X-Force report prepared by IBM Security says that 2016 is a record-breaking year in terms of information leakage[36]. As compared to 2015, the phenomenon of data leakage increased in 2016 by 566 percent. What is more, "70 percent of companies attacked by ransomware[37] paid at least 10 thousand dollars to regain access to their data"[38]. This fact specifically motivates criminals to carry out subsequent attacks.

---

31 *Bezpieczeństwo finansowe w bankowości elektronicznej…* op.cit., p. 35.

32 M. Kisiel, *Vishing – ulepszona metoda „na wnuczka"*, Bankier.pl (6.02.2015) http://www.bankier.pl/wiadomosc/Vishing-ulepszona-metoda-na-wnuczka-7236465.html (read on: 30 May 2017).

33 *Bezpieczeństwo finansowe w bankowości elektronicznej…* op.cit., p. 38.

34 Ibidem, p. 38.

35 Ibidem, p. 38.

36 Interia, 2016 as a record-breaking year in terms of data leakage, http://nt.interia.pl/internet/news-2016-rekordowym-rokiem-pod-wzgledem-wyciekow-danych,nId,2394177 (read on: 27 May 2017).

37 Type of software used for cybercrime purposes.

38 Ibidem.

3. Summary

Cybercriminals are increasingly trying to make use of gaps in the bank protection systems[39]. Kaspersky Lab, an anti-virus company, reported that at the end of Q3 2015 there were discovered as many as 5.6 million instances of violation relating to attempted theft of money from bank accounts[40].

A report published by mBank as part of the "Uważni w sieci" ("Prudent Network Users") campaign points out several important issues. A survey commissioned by mBank has shown that[41] 7 out of 10 Poles using the mobile banking feel safe online. What is more, 68% of the respondents say they cope well with the new technologies, while as many as 92% regards themselves as advanced users of the new solutions. On the other hand, 5 out of 10 Poles do not use anti-virus applications on their phones and do not update their operating system. The most alarming seems to be the fact that 1 in 3 users has logged in to their bank account from another (someone else's) computer[42]. Analysis of the presented results shows that cyberattacks can be blamed not only on cybercriminals but also on their victims. An old adage says that 'opportunity makes a thief'. Negligence on the part of users makes the task much easier for the fraudsters. Unfortunately, not everyone is aware of this. Therefore, (effective) counteracting cybercrime must be based on building a proper level of awareness of the rights and obligations resulting from the application of state--of-the-art technologies for using banking services.

If the above mentioned crimes are to be avoided, the following priority rules need to be complied with[43]: 1) "Never communicate any data necessary to log into electronic banking via e-mail/phone". 2) "Protect your computer and phone e.g. by software updates and antivirus software". 3) "Do not open any suspicious e-mails or attachments". 4) "Check whether the bank site is protected (encrypted connection, secure certificates)". 5) "Check the date of the last time you logged in to electronic banking". 6) "Create a strong, i.e. safe, password to your bank account, the one that is difficult to crack". 7) "Use secure WI-FI networks". 8) "Check the ATMs". 9) "Take care of your phone, i.e. never leave it logged into your bank account".

---

39 Newseria.pl, https://biznes.newseria.pl/news/rosnie_ryzyko,p215408645 (read on: 19 May 2017).

40 Kaspersky Lab, https://www.kaspersky.pl/o-nas/informacje-prasowe/2510/ponad-5-6-mln-prob-atakow-na-konta-bankowe-online-eksperci-z-kaspersky-lab-przeanalizowali-cyberzagrozenia-w-iii-kwartale-2015-r (read on: 19 May 2017).

41 An online study carried out in January 2016 among subjects aged 15-50 (including 270 persons having a bank account, computer and a smartphone, 341 persons using Internet banking and 130 persons using mobile banking).

42 mBank, *Korzystanie z bankowości elektronicznej a bezpieczeństwo w sieci*, https://www.mbank.pl/uwazniwsieci/page/raport/ (read on: 12 July 2017).

43 *Najlepsze konto*, *Bezpieczna bankowość elektroniczna*, http://www.najlepszekonto.pl/bezpieczna--bankowosc-15-praktycznych-porad (read on: 1 June 2017).

Given the increasing scale of the phenomenon, it should be noted that cybercrime is one of the biggest problems that the contemporary world has to face[44]. One needs to be aware that the universality and easy access to various types of information available on the Internet results in the fact that the list of threats to information security is still open, as the information society is constantly developing[45].

REFERENCES

[1] Babik W. (ed.), *Nauka o informacji*, the Polish Librarians' Association (SBP) Publishing House, Warszawa 2016, p. 368.

[2] Bogdalski P., Nowakowski Z., Płus T., Rajchel J., Rajchel K. (ed.), *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, The Police Academy in Szczytno (WSP w Szczytnie), Warszawa 2013, p. 329.

[3] Capiga M., *Bezpieczeństwo transakcji finansowych w Polsce*, CeDeWu, Warszawa 2015, p. 179.

[4] Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Siedlce University of Natural Science and Humanities (Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach), Siedlce 2016.

[5] Hajduk E., Hajduk M., *Wybrane aspekty związane z wykorzystaniem Internetu w biznesie*, [in:] *Komputer – przyjaciel czy wróg?*, Szewczyk A. (ed), The University of Szczecin (Uniwersytet Szczeciński), Faculty of Economics and Management, Institute of Computer Science in Management, Printshop Publishing House, Szczecin 2005, pp. 367-373.

[6] Kawiński A., Sieradz A. (ed.), *Wyzwania informatyki bankowej*, The Gdańsk Institute for Market Economics (Instytut Badań nad Gospodarką Rynkową), The Gdańsk School of Banking (Gdańska Akademia Bankowa), Gdańsk 2016.

[7] Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa,* [in:] "Telekomunikacja i Techniki Informacyjne" 2014, Vol. 1-2, p. 25.

[8] Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, [in:] "Przegląd Bezpieczeństwa Wewnętrznego", 2014, Vol. 10, pp. 108-111.

[9] Ministry of the Interior and Administration, *Rządowy Program Ochrony przed Cyberprzestępczością RP na lata 2011-2016 (The Government Program for the Protection of Cyberspace of the Republic of Poland for the years 2011-2016),* Warszawa 2010.

[10]. Oleksiewicz I., Krztoń W., *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Rambler Publishing House, Warszawa 2017.

[11]. Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)*, [in:] "ZIN Studia Informacyjne" (ZIN – Issues in Information Science. Information Studies) 2013, Vol. 2 (102), pp. 28-32.

[12]. Wawrzyniak D., *Bezpieczeństwo bankowości elektronicznej,* [in:] "Bankowość elektroniczna", Gospodarowicz A. (ed.), Polish Economic Publishing House (PWE), Warszawa 2005, p. 72 et seq.

[13]. Wojciechowska-Filipek S., *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010, p. 77 et seq,

[44] I. Oleksiewicz, W. Krztoń, *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Rambler Publishing House, Warszawa 2017.

[45] L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, Working Papers (Zeszyty Naukowe), Vol. 2(10)/2014, p. 230.

ELECTONICAL SOURCES

[1] Kisiel M., *Vishing – ulepszona metoda „na wnuczka"*, Bankier.pl 2015-02-06, http://www.bankier.pl/wiadomosc/Vishing-ulepszona-metoda-na-wnuczka-7236465.html (read on: 30 May 2017).

[2] Bednarek M., Wątor J., R*ządy, firmy, szpitale i szkoły na celowniku hakerów. Największy cyberatak w historii*, Wyborcza.pl 13 May 2017, http://wyborcza.pl/7,75399,21806893,rzady-firmy-szpitale-i-szkoly-na-celowniku-hakerow-najwiekszy.html (read on: 12 July 2017).

[3] *CERT*: *In 2016, cybercriminals most often tried to fraudulently obtain information,* http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1036280,cyberprzestepcy-najczesciej-probowali-wyludzic-informacje.html (read on: 12 July 2017).

[4] The Orange Foundation (Fundacja Orange), *Postrzeganie Internetu i nowych technologii w Polsce (Perception of the Internet and new technologies in Poland), Warszawa, Raport 2015 (2015 Report)*, p. 10. http://www.krrit.gov.pl/drogowskaz-medialny/aktualnosci/news,2123,postrzeganie-internetu-i-nowoczesnych-technologii-w-polsce.html (read on: 12 July 2017).

[5] http://nt.interia.pl/internet/news-2016-rekordowym-rokiem-pod-wzgledem-wyciekow-danych,nId,2394177 (read on: 27 May 2017).

[6] http://biznes.interia.pl/raport/bezpiecznie-w-sieci/news/phishing-czyli-rekordowo-wielkie-wyludzanie,2489719,8636 (read on: 30 May 2017).

[7] https://biznes.newseria.pl/news/rosnie_ryzyko,p215408645 (read on: 19 May 2017).

[8] https://www.kaspersky.pl/o-nas/informacje-prasowe/2510/ponad-5-6-mln-prob-atakow-na-konta-bankowe-online-eksperci-z-kaspersky-lab-przeanalizowali-cyberzagrozenia-w-iii-kwartale-2015-r (read on: 19 May 2017).

[9] https://www.mbank.pl/uwazniwsieci/page/raport/ (read on: 12 July 2017).

[10] http://www.najlepszekonto.pl/bezpieczna-bankowosc-15-praktycznych-porad (read on: 1 June 2017).

[11] http://www.pomorska.pl/strefa-biznesu/wiadomosci/z-kraju-i-ze-swiata/a/bankowosc-elektroniczna-jak-nie-dac-sie-okrasc-cyberprzestepcom,11409221/ (read on: 30 May 2017).