Marzena Hajduk-Stelmachowicz[1], Karolina Iwan[2]

Zarządzanie bezpieczeństwem informacji w obszarze bankowości elektronicznej wobec zjawiska cyberprzestępczości – aspekt indywidualny

1. Wstęp

Coraz więcej niepokoju budzą prezentowane w mediach incydenty cyberprzestępstw[3] mające miejsce niemalże w każdym zakątku świata[4].

Jak podaje portal Wyborcza.pl, w maju 2017 roku doszło do najpoważniejszego cyberataku w historii. „Na liście ofiar […] cyberprzestępców znajdują się m.in. rosyjski rząd, firma kurierska FedEx, szpitale w Wielkiej Brytanii, Indonezji i Korei Południowej, a także chińskie szkoły"[5]. W sumie cyberataków dokonano aż w 99 krajach. Zaatakowano między innymi rosyjskiego operatora telefonii komórkowej oraz banki[6]. Do ataku wykorzystano *ransomware*[7]. Po zainfekowaniu komputerów, domagano się zapłaty okupu w wysokości 300 dolarów. Ekspert ds. bezpieczeństwa Varum Badwhar przyznał, że nie zdarzyła się do tej pory sytuacja, w której rozprzestrzenienie ataku zajęłoby jedynie dobę[8].

---

1 Politechnika Rzeszowska, Wydział Zarządzania.

2 Politechnika Rzeszowska, Studenckie Koło Naukowe Młodych Ekonomistów.

3 Cyberprzestępstwa stanowią rodzaj czynów zabronionych popełnianych w cyberprzestrzeni. Por. Ministerstwo Spraw Wewnętrznych i Administracji, *Rządowy Program Ochrony przed Cyberprzestępczością RP na lata 2011–2016*, Warszawa 2010.

4 J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne" 2014, nr 1–2, s. 25.

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

6 Wyborcza.pl, http://wyborcza.pl/7,75399,21806893, rzady-firmy-szpitale-i-szkoly-na-celowniku-hakerow-najwiekszy.html (dostęp: 19.05.2017).

7 Złośliwe oprogramowanie, które szyfruje dane i blokuje do nich dostęp.

8 M. Bednarek, J. Wątor, op. cit.

W 2016 roku zespół CERT Polska zwalczał 1926 incydentów cyberzagrożeń[9]. W porównaniu do roku 2015 jest to wzrost o 32%[10]. Autorzy raportu wskazali, że „przestępcy posługują się szerokim wachlarzem rozwiązań, zwłaszcza w przypadku kradzieży oszczędności z wykorzystaniem urządzeń mobilnych"[11].

Przestępcy zawsze dokonują ataków hakerskich w sposób przemyślany. Szczególnie narażonyni na ataki cyberprzestępców są instytucje finansowe oraz ich klienci. Instutucje te są bogate w ogromne ilości cennych informacji[12]. Są także pożądane w kontekście wykorzystania ich zasobów do spekulacji finansowych[13]. Przykładem takich instytucji są na przykład banki eksploatujące obszar bankowości elektronicznej, który jest ściśle związany z cyberprzestrzenią[14]. Według badań „Postrzeganie Internetu i nowych technologii w Polsce" (przeprowadzonych przez Fundację Orange) wśród trzech obszarów życia, na które Internet i rozwój nowych technologii wpłynął najbardziej (w ciągu ostatnich 10 lat), pojawiło się wskazanie na[15]: załatwianie spraw finansowych, na przykład obsługi konta bankowego (44% odpowiedzi). Jest to zrozumiałe, bowiem bankowość elektroniczna zapewnia wygodę transakcji poprzez łatwy dostęp do środków pieniężnych (bez konieczności udawania się do placówki banku)[16]. Dzięki dynamice rozwoju oferuje coraz to nowsze i dogodniejsze rozwiązania dla klienta oraz samego banku.

---

[9] Incydenty można zgłaszać przez stronę CERT Polska: https://www.cert.pl/zglos-incydent/.

[10] *CERT: W 2016 r. cyberprzestępcy najczęściej próbowali wyłudzić informacje*, http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1036280, cyberprzestepcy-najczesciej-probowali-wyludzic-informacje.html (dostęp: 12.07.2017).

[11] Ibidem.

[12] Por. *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, P. Bogdalski, Z. Nowakowski, T. Płus, J. Rajchel, K. Rajchel (red.), WSP w Szczytnie, Warszawa 2013.

[13] Por. Z. Ciekanowski, J. Nowicka, H. Wyrębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016.

[14] Przez pojęcie cyberprzestrzeń należy rozumieć cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Por. *Rządowy Program Ochrony przed Cyberprzestępczością RP na lata 2011–2016*, Warszawa 2010.

[15] Fundacja Orange, *Postrzeganie Internetu i nowych technologii w Polsce*, Warszawa, Raport 2015, s. 10, http://www.krrit.gov.pl/drogowskaz-medialny/aktualnosci/news,2123, postrzeganie-internetu-i-nowoczesnych-technologii-w-polsce.html (dostęp: 12.07.2017).

[16] E. Hajduk, M. Hajduk, *Wybrane aspekty związane z wykorzystaniem Internetu w biznesie*, w: *Komputer – przyjaciel czy wróg?*, A. Szewczyk (red.), Uniwersytet Szczeciński, Wydział Nauk Ekonomicznych i Zarządzania, Instytut Informatyki w Zarządzaniu,Wydawnictwo Printshop, Szczecin 2005, s. 367–373.

Rozwijając i dogłębniej analizując pojęcie cyberataków, warto zwrócić uwagę na niebezpieczeństwa związane z obszarem e-bankowości. Głównym celem niniejszego artykułu było bowiem zaprezentowanie przykładów zagrożeń ze strony cyberprzestępców, które mogą dotknąć użytkowników bankowości elektronicznej. W pracy zwrócono uwagę na konieczność zarządzania informacją. Potraktowano ją jako potrzebę systematycznych działań (integrujących wiele interdyscyplinarnych zagadnień i problemów współczesnej nauki o informacji[17]) nie tylko w perspektywie organizacyjnej, ale także w perspektywie indywidualnej. Na takie podejście nade wszystko powinno kłaść się nacisk (jak wskazuje analiza literatury przedmiotu)[18]. W związku z realizacją celu pracy wykorzystano metodę, jaką jest analiza wybranej literatury przedmiotu.

2. Typologizacja przestępstw w obszarze bankowości elektronicznej

Wraz z postępem technologicznym liczba przestępstw stale wzrasta, a ich kontrolowanie staje się coraz trudniejsze nawet przez najwyższe organy państwowe[19]. Zagrożenia celowego zakłócenia prawidłowego funkcjonowania cyberprzestrzeni (bez konieczności angażowania personelu lub innych użytkowników), umożliwiające ominięcie lub osłabienie sprzętowych i progamowych mechanizmów kontroli dostępu[20], w sposób szczególny odnosi się do usług bankowości elektronicznej. Cyberataki mogą mieć bowiem miejsce zarówno po stronie serwera, jak i klienta (rysunek 1).

Raport *Krajobraz bezpieczeństwa polskiego Internetu 2016 r.* wykazał, że CERT Polska[21] otrzymał ponad 722 tys. zgłoszeń dotyczących phishingu. Jak podaje portal Interia Biznes, „podszywanie się pod instytucje finansowe, operatorów telekomunikacyjnych, banki, firmy telekomunikacyjne w celu wyłudzenia danych, loginów i haseł do kont, czyli phishing, był jednym z największych

[17] B. Sosińska-Kalata, *Obszary badań współczesnej informatologii (nauki o informacji)*, „ZIN Studia Informacyjne. Information Studies" 2013, nr 2 (102), s. 28–32.

[18] *Nauka o informacji*, W. Babik (red.), Wydawnictwo SBP, Warszawa 2016, s. 368.

[19] Według firmy Control Risks ok. 33% cyberataków w 2016 r. skierowano przeciwko sektorowi publicznemu.

[20] Por. *Rządowy Program Ochrony przed Cyberprzestępczością RP na lata 2011–2016*.

[21] CERT Polska (ang. *Computer Emergency Response Team*) jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo użytkowników lub instytucji w internecie. Działa od 1996 r. przy NASK (Naukowej i Akademickiej Sieci Komputerowej).

zagrożeń bezpieczeństwa 2016 roku. Obecny rok zapowiada się pod względem phishingu jako rekordowy"[22].

Wyłudzanie poufnych informacji osobistych[23] oparte jest na przesyłaniu wiadomości z adresem strony internetowej przez przestępców podszywających się pod na przykład instytucję finansową[24]. Przesłany adres strony internetowej w znacznym stopniu przypomina dostęp do oryginalnej strony banku[25].

Przestępcy zachęcając do wejścia na fałszywą stronę, wskazują na potrzebę kliknięcia załączonego w e-mailu linku. Konieczność podjęcia działania argumentują między innymi przedłużeniem ważności karty, jej aktywacją lub poprawą bezpieczeństwa jej użytkowania. Po wpisaniu przez mało czujnego klienta żądanych danych, przestępcy uzyskują możliwość dokonywania przelewów na założone przez siebie konta[26]. Profesjonalizm cyberprzestępców sprawia, że czasami należy poświęcić sporo czasu, aby zauważyć różnice w adresach domenowych[27]. W kontekście zwiększenia bezpieczeństwa transakcji w sieci istotnym aspektem jest upewnianie się, że dana strona internetowa posiada „szyfrowane połączenie z serwerem" (adres rozpoczyna się od „https", a obok niego znajduje się ikona zamkniętej kłódki)[28].

---

[22] Interia Biznes, *Phishing czyli rekordowe wielkie wyłudzenie*, http://biznes.interia.pl/raport/bezpiecznie-w-sieci/news/phishing-czyli-rekordowo-wielkie-wyludzanie,2489719,8636 (dostęp: 30.05.2017).

[23] M. Capiga, *Bezpieczeństwo transakcji finansowych w Polsce*, CeDeWu, Warszawa 2015, s. 179, za: S. Wojciechowska-Filipek, *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010.

[24] S. Wojciechowska-Filipek, op. cit., s. 77 i nast.

[25] D. Wawrzyniak, *Bezpieczeństwo bankowości elektronicznej*, w: *Bankowość elektroniczna*, A. Gospodarowicz (red.), PWE, Warszawa 2005, s. 72 i nast.

[26] *Bezpieczeństwo finansowe w bankowości elektronicznej– przestępstwa finansowe związane z bankowością elektroniczną*, M. Górnisiewicz (red.), Komisja Nadzoru Finansowego, CEDUR, Warszawa 2014, s. 40.

[27] Por. *Wyzwania informatyki bankowej*, A. Kawiński, A. Sieradz (red.), Instytut Badań nad Gospodarką Rynkową, Gdańska Akademia Bankowa, Gdańsk 2016.

[28] 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/ (dostęp: 30.05.2017).

Wspólne dla serwera oraz klienta źródła zagrożeń Bazują na podsłuchiwaniu i modyfikacji danych przesyłanych sieciami	• **sniffing** – podsłuchiwanie, • **spoofing** – podszywanie się pod inny komputer w sieci, • **network snooping** – wstępne rozpoznawanie parametrów sieci przede wszystkim pod kątem bezpieczeństwa, • **vishing** – podszywanie się przestępcy pod bank po to, aby wyłudzić pin i login do bankowości elektonicznej klienta, • **phishing** – wyłudzanie poufnych informacji osobistych, • **ataki typu *man-in-the-midle***, odmiana phishingu w przypadku której przestępca komunikuje się za pomocą sfałszowanej strony interentowej, • **ataki typu *man-in-the-browser***, polegajace na ataku na przeglądarki internetowe, • **sabotaż komputerowy i cyberterroryzm**, • **zagrożenia usług STMP, MIME, POP** i inne, • **zagrożenia DNS** bazujące głównie na podatności usługi na ataki typu denial of service.
Zagrożenia dotyczace klienta Związane z procedurami logowania się systemu oraz pracy z oprogramowaniem klienta	• zagrożenia kompromitacji parametrów dostępu do systemu, takich jak identyfikator oraz hasło, • manipulacja w obrębie softweru oraz hadrweru, mająca na celu zmiany ich funkconalności niewidoczne dla użytkownika, • błędy w oprogramowaniu standardowym, np. przeglądarkach internetowych, • błędy w oprogramowaniu niestandardowym, • wirusy – samoistnie powielające się programy komputerowe o szkodliwym działaniu.
Zagrożenia serwera Obejmują ataki na zasoby serwera	• ataki blokujące DoS oraz DDoS. Ich kwintesencją jest atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów (przeprowadzony równocześnie z jednego lub wielu komputerów), • ataki z wykorzystaniem specjalnych programów (np. wirusów, koni trojańskich, bomb logicznych), które umożliwiają ingerencję w systemy informatyczne, bazy danych, • zagrożenia wynikające ze zdarzeń losowych oraz środowiskowych (np. pożary, wyładowania atmosferyczne, powodzie), • zagrożenia wynikajace z niestaranności, błędów, zaniedbań, nielojalności i nieuczciwości personelu.

Rysunek 1. Przykłady zagrożeń występujących w obszarze bankowości elektronicznej

Źródło: opracowanie własne na podstawie: M. Capiga, op. cit., s. 77 i nast.; D. Wawrzyniak, *Bezpieczeństwo bankowości elektronicznej*, w: *Bankowość elektroniczna*, A. Gospodarowicz (red.), PWE, Warszawa 2005, s. 72 i nast.

Kolejnym przykładem przestępstwa w obszarze bankowości elektronicznej jest tzw. **skimming**. Polega on na skopiowaniu informacji zawartych na pasku magnetycznym karty płatniczej[29]. Możemy wyróżnić jego dwa rodzaje[30]:

- skimming bankomatowy – polega na dokonaniu modyfikacji w budowie bankomatu w celu skopiowania danych i utworzenia duplikatu karty;
- skimming w punktach usługowo-handlowych – polega na przechwyceniu danych w momencie dokonywania transakcji przez właściciela karty.

Podstawową czynnością w przypadku skimmingu bankomatowego jest zainstalowanie w bankomacie urządzenia skanującego (skimmera) dane z karty płatniczej. Urządzania takie pozwalają zarówno na wysyłanie przejętych danych drogą radiową na komputer przestępcy, jak i na bezpośrednie ich zapamiętywanie na karcie pamięci, którą posiadają. Z punktu widzenia przestępcy najważniejsze jest zeskanowanie paska magnetycznego karty płatniczej. „Pasek magnetyczny oryginalnej karty płatniczej zawiera trzy ścieżki: na pierwszej zapisane w formie jawnej jest imię i nazwisko posiadacza karty, suma kontrolna, dane kraju i banku wydającego kartę, na drugiej znajduje się numer karty, data ważności i kod serwisowy do prawidłowego odczytu, trzecia ścieżka pozostaje praktycznie niewykorzystana"[31].

Kolejnym istotnym etapem ataku jest zainstalowanie niewielkiej kamerki oraz umieszczenie na klawiaturze bankomatu tzw. nakładki pozwalającej na zapamiętywanie poszczególnych cyfr PIN-u i zapisywanie ich w odpowiedniej kolejności na czytniku. Po uzyskaniu wszystkich niezbędnych informacji, przestępcy są w stanie zarządzać kartą i dostępnymi na niej środkami finansowymi. W przypadku skimmingu w punktach usługowo-handlowych dane z karty skanowane są na przykład przez sprzedawcę, który współpracuje z hakerami bądź sam nim jest. Skopiowanie paska magnetycznego nie jest zbyt trudne, ponieważ wystarczy przyłożyć kartę do urządzania skanującego o niewielkich wymiarach. Następnie przejęte dane z paska magnetycznego przenoszone są na „czystą kartę magnetyczną" lub na oryginalną kartę płatniczą (bardzo często ukradzioną).

Powszechnym działaniem służącym do przeprowadzania ataków jest także **spoofing**. Przestępcy poprzez przejęcie kontroli nad komputerem innego użytkownika wykorzystują go w celach bezprawnych działań[32]. Coraz bardziej popularne stają się akcje oparte na **vishingu**, kiedy to oszuści podszywają się pod bank

[29] M. Capiga, op. cit., s. 179.

[30] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, t. 6, nr 10, s. 108–111.

[31] Ibidem, s. 110.

[32] *Bezpieczeństwo finansowe w bankowości elektronicznej…*, s. 35.

i na przykład przez kontakt telefoniczny dążą do wyłudzenia loginu lub hasła. Akcję opartą na vishingu wykorzystali w 2015 roku członkowie gangu działającego na terenie Wielkiej Brytanii. Dzwonili oni do przypadkowo wybranych ofiar, podając się za policjantów i prosząc o wydanie karty w związku ze śledztwem dotyczącym rzekomych włamań na rachunki bankowe. „Po wyrażeniu zgody przez ofiarę, do jej drzwi pukali «policyjni kurierzy», którzy odbierali karty"[33]. Przejęte karty natychmiastowo oczyszczano ze wszystkich środków finansowych.

Przeprowadzane ataki niemal zawsze opierają się na działaniu złośliwych oprogramowań, do których zaliczyć można popularne wirusy komputerowe, bomby logiczne, robaki komputerowe oraz konie trojańskie, tzw. trojany. Wirusy komputerowe to programy, które umieszczone są w innym programie i mają zdolność powielania się. Ich działanie może doprowadzić do między innymi kasowania się danych, kradzieży danych czy też zatrzymania pracy danego komputera[34]. Podobnym działaniem charakteryzuje się robak komputerowy, jednak „w przeciwieństwie do wirusa komputerowego nie niszczy danych i nie przekształca plików, ale może prowadzić do obciążenia programów komputerowych […], powodując znaczne utrudnienia lub uniemożliwienie korzystania z nich"[35].

Istotne i często długo niezauważane zagrożenie stanowią tzw. bomby logiczne, które mogą „pozostać w ukryciu przez długi czas, a ich aktywacja następuje w momencie nadejścia określonej daty lub wykonania przez użytkownika określonej czynności"[36].

Raport IBM X-Force 2017 sporządzony przez firmę IBM Security wykazał, że rok 2016 jest rokiem rekordowym pod względem wycieków informacji[37]. W porównaniu do roku 2015 zjawisko wycieku danych wzrosło o 566% w roku 2016. Co więcej, „70 proc. firm zaatakowanych przy użyciu ransomware[38] zapłaciło przynajmniej 10 tys. dolarów, by odzyskać dostęp do swoich danych"[39]. Fakt ten w sposób szczególny motywuje cyberprzestępców do dokonywania kolejnych ataków.

---

[33] M. Kisiel, *Vishing – ulepszona metoda „na wnuczka"*, http://www.bankier.pl/wiadomosc/Vishing-ulepszona-metoda-na-wnuczka-7236465.html (dostęp: 30.05.2017).

[34] *Bezpieczeństwo finansowe w bankowości elektronicznej…*, s. 38.

[35] Ibidem, s. 38.

[36] Ibidem, s. 38.

[37] Interia, *2016 rekordowym rokiem pod względem wycieków danych*, http://nt.interia.pl/internet/news-2016-rekordowym-rokiem-pod-wzgledem-wyciekow-danych,nId,2394177 (dostęp: 27.05.2017).

[38] Rodzaj oprogramowania używanego w przestępczości internetowej (ang. *ransom* – okup).

[39] Interia, *2016 rekordowym rokiem pod względem wycieków danych*, http://nt.interia.pl/internet/news-2016-rekordowym-rokiem-pod-wzgledem-wyciekow-danych,nId,2394177 (dostęp: 27.05.2017).

3. Podsumowanie

Cyberprzestępcy coraz częściej starają się wykorzystywać luki w zabezpieczeniach bankowych[40]. Firma antywirusowa Kaspersky Lab odnotowała, że pod koniec III kwartału 2015 roku wykryto aż 5,6 mln naruszeń dotyczących prób kradzieży środków pieniężnych z kont bankowych[41].

W raporcie opublikowanym przez mBank w ramach akcji „Uważni w sieci" zwrócono uwagę na kilka istotnych kwestii. Przeprowadzone na polecenie mBanku badanie[42] wykazało, że 7 na 10 Polaków korzystających z bankowości mobilnej czuje się w sieci bezpiecznie. Co więcej, 68% badanych uważa się za osoby, które dobrze radzą sobie z nowymi technologiami, a aż 92% uważa się za zaawansowanych użytkowników nowych rozwiązań. Tymczasem 5 na 10 Polaków nie stosuje aplikacji antywirusowej na swoim telefonie oraz nie aktualizuje systemu operacyjnego. Najbardziej niepokojący wydaje się fakt, że 1 na 3 użytkowników logował się na swoje konto bankowe z innych (obcych) komputerów[43].

Na podstawie analizy przedstawionych wyników zauważyć można, że wina za występowanie cyberataków leży nie tylko po stronie cyberprzestępców, ale także i ich ofiar. Jak poucza przysłowie: okazja czyni złodzieja. Zaniedbania ze strony użytkowników znacznie ułatwiają oszustom ich działania. Niestety, nie każdy ma tego świadomość. Dlatego też przeciwdziałanie cyberprzestępczości (aby było skuteczne) musi być oparte na budowaniu właściwego poziomu świadomości praw i obowiązków wynikających ze stosowania nowoczesnych technologii w zakresie korzystania z usług bankowych.

W celu ustrzeżenia się przed omówionymi przestępstwami należy przestrzegać kilku priorytetowych zasad[44]:

---

[40] Newseria.pl, https://biznes.newseria.pl/news/rosnie_ryzyko,p215408645 (dostęp: 19.05.2017).

[41] 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 (dostęp: 19.05.2017).

[42] Badanie online, realizowane w styczniu 2016 r., gdzie badaniu poddano osoby w wieku 15–50 lat (w tym 270 osób posiadających konto, komputer i smartfon, 341 osób korzystających z bankowości internetowej, 130 osób korzystających z bankowości mobilnej).

[43] mBank, *Korzystanie z bankowości elektronicznej a bezpieczeństwo w sieci*, https://www.mbank.pl/uwazniwsieci/page/raport/ (dostęp: 12.07.2017).

[44] *Najlepsze konto*, *Bezpieczna bankowość elektroniczna*, http://www.najlepszekonto.pl/bezpieczna-bankowosc-15-praktycznych-porad (dostęp: 01.06.2017).

1) Nie wolno podawać danych niezbędnych do logowania do bankowości elektronicznej przez e-mail/telefon.
2) Należy zabezpieczać komputer i telefon przez na przykład aktualizację oprogramowania i programy antywirusowe.
3) Nie otwierać podejrzanych e-maili i załączników.
4) Należy sprawdzać zabezpieczenia strony banku (szyfrowane połączenie, certyfikat bezpieczeństwa).
5) Sprawdzać datę ostatniego logowania do bankowości elektronicznej.
6) Stworzyć trudne do rozszyfrowania tzw. bezpieczne hasło do konta bankowego.
7) Korzystać z bezpiecznych sieci Wi-Fi.
8) Sprawdzać bankomaty.
9) Dbać o swój telefon, nie pozostawiając go na przykład zalogowanego do konta bankowego.

Biorąc pod uwagę rosnącą skalę zjawiska, można stwierdzić, że cyberprzestępczość to jeden z największych problemów, z jakim przyszło się zmierzyć współczesnemu światowi. Należy mieć świadomość, że powszechność i łatwy dostęp do różnego rodzaju informacji za pomocą Internetu sprawiają, że katalog zagrożeń dla bezpieczeństwa informacji jest ciągle otwarty, gdyż społeczeństwo informacyjne stale się rozwija[45].

Bibliografia

Capiga M., *Bezpieczeństwo transakcji finansowych w Polsce*, CeDeWu, Warszawa 2015, s. 179.

Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016.

Hajduk E., Hajduk M., *Wybrane aspekty związane z wykorzystaniem Internetu w biznesie*, w: *Komputer – przyjaciel czy wróg?*, A. Szewczyk (red.), Uniwersytet Szczeciński, Wydział Nauk Ekonomicznych i Zarządzania, Instytut Informatyki w Zarządzaniu,Wydawnictwo Printshop, Szczecin 2005, s. 367–373.

Wyzwania informatyki bankowej, A. Kawiński, A. Sieradz (red.), Instytut Badań nad Gospodarką Rynkową, Gdańska Akademia Bankowa, Gdańsk 2016.

[45] L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, „Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2014, nr 2(10), s. 230.

Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne" 2014, nr 1–2, s. 25.

Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, t. 6, nr 10, s. 108–111.

Ministerstwo Spraw Wewnętrznych i Administracji, *Rządowy Program Ochrony przed Cyberprzestępczością RP na lata 2011–2016*, Warszawa 2010.

Nauka o informacji, W. Babik (red.), Wydawnictwo SBP, Warszawa 2016, s. 368.

Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)*, „ZIN Studia Informacyjne. Information Studies" 2013, nr 2(102), s. 28–32.

Więcaszek-Kuczyńska L., *Zagrożenia bezpieczeństwa informacyjnego*, „Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2014, nr 2(10).

Wawrzyniak D., *Bezpieczeństwo bankowości elektronicznej*, w: *Bankowość elektroniczna*, A. Gospodarowicz (red.), PWE, Warszawa 2005, s. 72 i nast.

Wojciechowska-Filipek S., *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010, s. 77 i nast.

Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski, P. Bogdalski, Z. Nowakowski, T. Płus, J. Rajchel, K. Rajchel (red.), WSP w Szczytnie, Warszawa 2013, s. 329.

Źródła sieciowe

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

CERT: W 2016 r. cyberprzestępcy najczęściej próbowali wyłudzić informacje, http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1036280, cyberprzestepcy-najczesciej-probowali-wyludzic-informacje.html (dostęp: 12.07.2017).

Fundacja Orange, *Postrzeganie Internetu i nowych technologii w Polsce, Warszawa, Raport 2015*, s. 10, http://www.krrit.gov.pl/drogowskaz-medialny/aktualnosci/news,2123, postrzeganie-internetu-i-nowoczesnych-technologii-w-polsce.html (dostęp: 12.07.2017).

http://nt.interia.pl/internet/news-2016-rekordowym-rokiem-pod-wzgledem-wyciekow-danych,nId,2394177 (dostęp: 27:05.2017).

http://biznes.interia.pl/raport/bezpiecznie-w-sieci/news/phishing-czyli-rekordowo-wielkie-wyludzanie,2489719,8636 (dostęp: 30.05.2017).

https://biznes.newseria.pl/news/rosnie_ryzyko,p215408645 (dostęp: 19.05.2017).

Kisiel M., *Vishing – ulepszona metoda „na wnuczka"*, Bankier.pl 2015–02–06, http://www.bankier.pl/wiadomosc/Vishing-ulepszona-metoda-na-wnuczka-7236465.html (dostęp: 30.05.2017).

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 (dostęp:19.05.2017).

https://www.mbank.pl/uwazniwsieci/page/raport/ (dostęp: 12.07.2017).

http://www.najlepszekonto.pl/bezpieczna-bankowosc-15-praktycznych-porad (dostęp: 01.06.2017).

http://www.pomorska.pl/strefa-biznesu/wiadomosci/z-kraju-i-ze-swiata/a/bankowosc-elektroniczna-jak-nie-dac-sie-okrasc-cyberprzestepcom,11409221/ (dostęp: 30.05.2017).

* * *

Information Security Management in Electronic Banking Considering the Phenomenon of Cybercrime

Summary

The subject of the elaboration is the issues of information security management in electronic banking. It draws attention to the growing phenomenon of cybercrime and its strong impact on the area of e-banking (from an individual point of view). The main aim of the article was to present the different types of threats that today's electronic banking users encounter.

Keywords: information security, e-banking, cybercrime.