METODY KONTROLI DOSTĘPU W BANKOWOŚCI ELEKTRONICZNEJ

Sylwia WOJCIECHOWSKA-FILIPEK

Streszczenie: Wykorzystanie technologii informacyjno-komunikacyjnych umożliwił zupełnie nowy sposób prowadzenia biznesu – mniej kosztowny, bardziej elastyczny o globalnej skali działania. Korzyści zarówno dla organizacji jak i dla klientów są tak duże, że praktycznie każda organizacja stara się maksymalnie wykorzystać nowe możliwości. Bankowość była i jest branżą, która najwięcej inwestuje w nowe technologie. Dla osiągnięcia pełnych efektów wynikających z wirtualizacji działalności potrzebne jest przezwyciężenie głównej bariery rozwoju zdalnej bankowości jaką są obawy o bezpieczeństwo zgromadzonych na koncie środków, czyli obawa, że osoba nieupoważniona mogłaby mieć do nich dostęp. Z tego też powodu banki stosują coraz to nowsze i pewniejsze metody kontroli dostępu. Na rynku obok najbardziej zaawansowanych metod takich jak podpisy cyfrowe czy urządzenia biometryczne nadal funkcjonują proste hasła i podpis odręczny. Celem niniejszego opracowania jest analiza metod kontroli dostępu wykorzystywanych w bankowości elektronicznej.

Słowa kluczowe: bankowość elektroniczna, bezpieczeństwo, identyfikacja, uwierzytelnianie, autoryzacja, biometria.

1. Kanały dostępu do produktów i usług bankowości elektronicznej

1.1. Istota bankowości elektronicznej

Bankowość z uwagi na swój specyficzny charakter działalności była sferą przodującą w wykorzystaniu technologii informacyjnej do usprawnienia przepływu informacji.

„Produkty finansowe z samej swojej istoty są predestynowane do istnienia na rynku elektronicznym. Łatwo poddające się dematerializacji, abstrakcyjne, związane są głównie z wymianą informacji" [1].

Rozwój IT determinował rozwój usług bankowych i sposób ich świadczenia. Bankowość elektroniczna jest bardzo innowacyjnym segmentem bankowości. Innowacyjność ta wynika z możliwości wykorzystywania nowych rozwiązań informacyjno - komunikacyjnych zarówno w produktach i usługach bankowych jak też w samej organizacji.

Bankowość elektroniczna to „kompleks usług i narzędzi o zróżnicowanym charakterze finansowym i organizacyjnym, udostępniany szeroko pojętemu klientowi sfery bankowej, oparty o najnowocześniejsze techniki informatyczno-komunikacyjne, zintegrowany z konglomeratem tradycyjnych systemów informatycznych wspomagających zarządzanie bankiem" [2].

1.2. Kanały dostępu do usług bankowych

Ze względu na kanał komunikacji bankowość elektroniczną można podzielić na:

- bankowość telefoniczną - usługi bankowe, w których kontakt banku z klientem następuje za pomocą telefonu stacjonarnego bądź telefonu komórkowego,
- bankowość mobilną (ang. *m-banking)* która pojawiła się wraz z możliwością dostępu do banku za pomocą telefonu komórkowego, pejdżerów i innych urządzeń komunikacji radiowej [3],
- bankowość terminalową (samoobsługową) – dostęp do rachunku bankowego oraz dokonywanie transakcji przy użyciu elektronicznych urządzeń takich jak bankomaty czy elektroniczne terminale [4],
- dedykowaną bankowość komputerową – komunikacja z bankiem za pośrednictwem modemu i specjalnego oprogramowania po stronie klienta,
- bankowość internetową - wszelkie usługi banku, których funkcjonowanie oparte jest w swojej istocie na wykorzystaniu sieci. Jest to zatem całokształt działalności rynkowej banku w wirtualnej, tworzonej przez internetową komunikację, przestrzeni [3].

2. Bezpieczeństwo bankowości elektronicznej

2.1. Źródła zagrożeń

Bezpieczeństwo jest decydującym czynnikiem rozwoju e-commerce, a zwłaszcza zdalnych kanałów dostępu do „wrażliwych" usług finansowych [5]. Zgodnie z badaniem przeprowadzonym przez CBOS w 2008 roku, aż 80% Polaków nie było przekonanych o bezpieczeństwie bankowości elektronicznej [6].

Bezpieczeństwo w znaczeniu informatycznym to pewien stan, który charakteryzuje się określonym poziomem najważniejszych atrybutów takich jak [7, 8]:

- poufność – gwarantującą, że dostęp do danych przechowywanych i przetwarzanych w systemie mają tylko osoby do tego uprawnione,
- integralność – gwarantującą, że dane przesyłane w czasie transakcji elektronicznej nie są przez nikogo modyfikowane,
- autentyczność – pozwalająca stwierdzić, czy osoba podpisująca się pod transakcją jest rzeczywiście osobą, za którą się podaje,
- niezaprzeczalność – niepozwalajacą wyprzeć się faktu nadania lub odbioru komunikatu drogą elektroniczną,
- dostępność – gwarancja stałego dostępu do systemu bankowości elektronicznej opartego na autoryzowanym dostępie do tychże danych,
- niezawodność – gwarantującą, że system działa w sposób, jakiego się od niego oczekuje.

Odnosząc się do wymienionych atrybutów bezpieczeństwa można - upraszczając nieco problem – odnieść potencjalne zagrożenia bankowości elektronicznej do koncepcji czterech typów ataku na system informatyczny:

- przerwanie – zagrożenia dostępności,
- przechwycenie – zagrożenia poufności,
- modyfikacja – zagrożenia integralności,
- podrobienie – zagrożenia autentyczności.

Do najpopularniejszych obecnie ataków należą [9]:

- *Skimming* - polega na nielegalnym skopiowaniu zawartości paska magnetycznego karty płatniczej bez wiedzy jej posiadacza w celu wytworzenia kopii i wykonywania nieuprawnionych płatności za towary i usługi, lub wypłat z bankomatów. Istnieją dwa rodzaje *skimmingu: skimming* w placówce handlowej oraz *skimming* bankomatowy. Znacznie bardziej niebezpieczny jest *skimming* bankomatowy, polegający na tym, że przestępcy instalują na bankomatach lub w ich wnętrzu specyficzne urządzenia, które służą do pozyskiwania danych z paska magnetycznego (czytnik) oraz PIN-u (kamera lub fałszywa klawiatura).
- *Phishing (łowienie haseł*) - polega na zmuszeniu użytkownika do wejścia na sfałszowaną stronę, na której cyberprzestępca przechwytuje dane potrzebne do autoryzacji. Może to być login i hasło użytkownika, ale również cała lista kodów jednorazowych z karty-zdrapki.
- *Man-in-the-middle* (*człowiek pośrodku*) – atak polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy.
- *Man-in-the-browser* (*człowiek w przeglądarce*) – ataki mogą, lecz nie muszą być powiązane ze ściągnięciem złośliwego oprogramowania i przez to są najniebezpieczniejsze. Z wykorzystaniem dobrze przygotowanego złośliwego oprogramowania można tak naprawdę wykonać wszelkie czynności na komputerze ofiary. Dzięki temu można przedstawić poprawność certyfikatów, można podsłuchać hasła, można również podmienić dane, które trafiają do podpisu elektronicznego. Ten atak opiera się większości metod dostępnych na rynku.

2.2. Kategorie środków ochrony

Zagrożenia jakie niesie ze sobą świadczenie usług bankowych na odległość powoduje u klientów brak zaufania do elektronicznej bankowości oraz obawy o bezpieczeństwo swoich środków, co stanowi jedną z głównych barier rozwoju zdalnych usług bankowych. Tymczasem zabezpieczenia stosowane przez polskie banki należą do jednych z najbardziej zaawansowanych. Można wyróżnić kilka kategorii środków ochrony [7]:

- Prawne - wszelkie unormowania prawne, które dotyczą ochrony danych przetwarzanych w bankowych systemach informatycznych.
- Fizyczne – zabezpieczenia funkcjonujące w otoczeniu systemu informacyjnego nie stanowiące jego części (urządzenia przeciwwłamaniowe, sejfy, alarmy itp.).
- Techniczne - rozwiązania sprzętowe związane z informatyką bądź wykorzystujące technologie informatyczne i w bezpośredni sposób wpływające na bezpieczeństwo systemu [10] (np. urządzenia podtrzymujące zasilanie, karty, urządzenia wykorzystywane do tworzenia kopii zapasowych wraz z metodami ich stosowania, serwery Proxy, sprzętowe blokady dostępu do klawiatur, napędów dysków itp.).
- Programowe - wszelkie rozwiązania zabezpieczające, dostępne dzięki wykorzystaniu oprogramowania zarówno systemowego jak i aplikacyjnego (np. dzienniki systemowe, programy śledzące, mechanizmy rozliczania, oprogramowanie antywirusowe, oprogramowanie antyspamowe itp.) [7, 11].
- Organizacyjne - dotyczą kontroli zarządzania i procedur bezpieczeństwa (analiza ryzyka, polityka bezpieczeństwa).
- Kryptograficzne - Kryptografią nazywamy naukę o metodach przesyłania wiadomości w zamaskowanej postaci, tak aby tylko odbiorca był w stanie odczytać wysłaną

przez nadawcę wiadomość, będąc jednocześnie pewnym, że nie została ona przez nikogo zmodyfikowana [7].

– Kontroli dostępu.

3. Środki kontroli dostępu

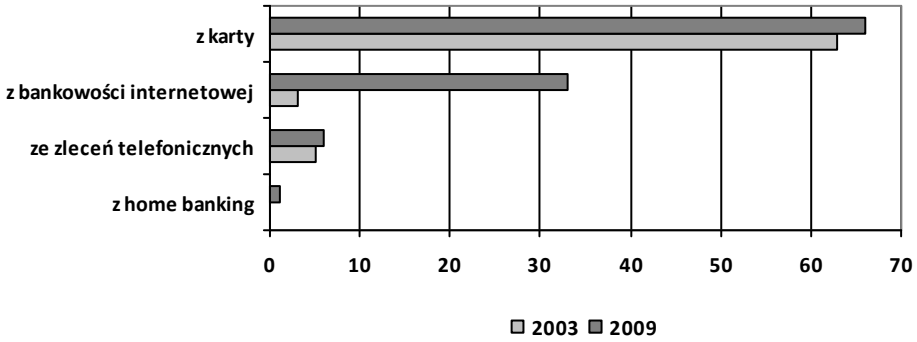
Identyfikacja, uwierzytelnianie i autoryzacja to trzy niezależne, lecz spokrewnione i mocno zakorzenione pojęcia środków kontroli dostępu [3]:

– *identyfikacja* - ustala, kim użytkownik jest,
– *uwierzytelnianie* – próbuje ustalić, że użytkownik jest tym, za kogo się podaje,
– *autoryzacja* – ustala, co użytkownikowi wolno zrobić w danej chwili.

Kontrola dostępu do sytemu i kontrola przysługujących użytkownikowi praw do wykonania danej operacji polega na uwierzytelnieniu użytkownika przez system. Uwierzytelnianiem podmiotu nazywamy proces, w trakcie którego jedna strona jest zapewniana (poprzez uzyskanie poświadczenia potwierdzającego) o tożsamości drugiej ze stron. Termin uwierzytelnianie podmiotu i identyfikacja są używane zamiennie.

Kontrola dostępu do systemu polega na uwierzytelnieniu użytkownika (człowiek, komputer, terminal, karta sprzętowa), którego dokonuje inny użytkownik poprzez analizę charakterystycznych cech. Możemy wyróżnić cztery podstawowe metody uwierzytelniania [12]:

– *weryfikacja wiedzy użytkownika* (ang. *by something you know - SYK*) – na podstawie tego, co użytkownik zna,
– *weryfikacja przedmiotu posiadanego przez użytkownika* (ang. *by something you have - SYH*) - na podstawie tego, co użytkownik ma,
– *weryfikacja cech fizycznych użytkownika* (ang. *by something you are - SYA*) – na podstawie tego, kim (czym) użytkownik jest,
– *weryfikacja czynności wykonywanych przez użytkownika* (ang. *by something you do - SYD*) - na podstawie tego, co użytkownik robi.



Rys.1. Korzystanie z elektronicznych kanałów dostępu przez posiadaczy ROR [13]

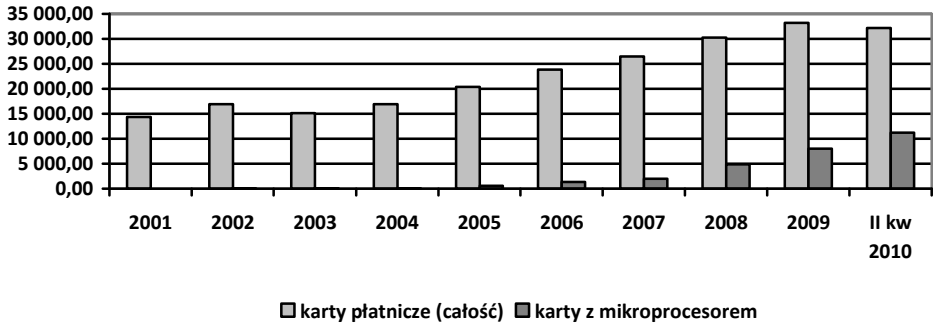
Najczęściej klienci korzystają z dostępu do środków finansowych zgromadzonych na koncie poprzez karty płatnicze oraz Internet (Rys. 1), dlatego też w dalszej części zostaną omówione środki kontroli dostępu poprzez te dwa główne kanały komunikacji z bankiem.

3.1. Kontrola dostępu przy korzystaniu z kart płatniczych

3.1.1. Zabezpieczenia transakcji bezgotówkowych wykonywanych kartami

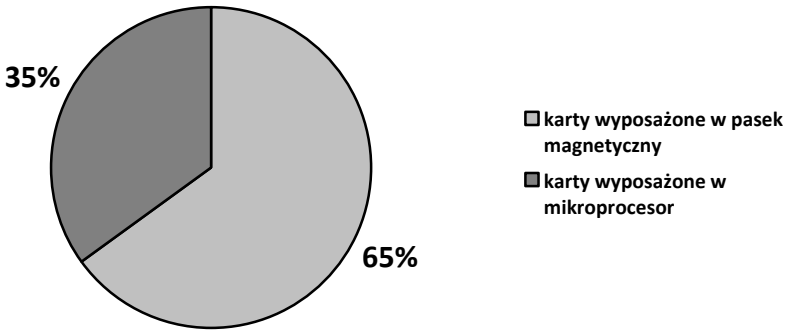
Metody kontroli dostępu do środków finansowych poprzez karty płatnicze zależą od rodzaju urządzenia, w którym przeprowadzana jest transakcja jak i od budowy samej karty:

1. *W imprinterach* - identyfikacja użytkownika następuje poprzez jego podpis dokonany własnoręcznie w obecności np. sprzedawcy a następnie porównaniu go z podpisem na karcie. Dodatkowo ważność karty sprawdza się poprzez bankowy wykaz numerów zastrzeżonych bądź przez telefon z najbliższym centrum autoryzacyjnym.
2. *W elektronicznych terminalach*:
   - *Karty z paskiem magnetycznym* - identyfikacja posiadacza odbywa się na zasadzie porównania wprowadzonego przez niego kodu PIN z tym, co jest przechowywane na pasku magnetycznym. Operacje na kartach magnetycznych dokonywane są przeważnie w trybie rzeczywistym (on line). PIN to praktycznie jedyne elektroniczne zabezpieczenie karty magnetycznej. Pozostałe mają charakter organizacyjny (dane wydrukowane na karcie, hologramy, mikrodruki, zdjęcie oraz podpis posiadacza i in.).
   - *Karty elektroniczne* - zapewniają możliwość zapisania znacznych ilości danych co pozwala na rozszerzenie zarówno zakresu kontroli autentyczności karty, jak i zdolności jej posiadacza do dokonania zamierzonej transakcji. Karty te są bardzo bezpiecznym instrumentem płatności z bardzo ograniczonymi możliwościami kopiowania i dodatkowymi elementami uwierzytelniania posiadacza jak kod PIN [14]. Karty te charakteryzują się bezpieczną kontrolą dostępu, możliwością szyfrowania i deszyfrowania informacji, a także generowania i weryfikacji podpisów cyfrowych. Nowoczesne standardy implementacji technologii mikroprocesorowej gwarantują także odporność kart na kopiowanie [7].



Rys. 2. Liczba kart bankowych w Polsce (w tys.)

W celu zminimalizowania przestępczości i zwiększenia zaufania klientów, europejskie banki rozpoczęły proces modyfikacji funkcjonujących rozwiązań. Przede wszystkim następuje migracja kart do ujednoliconego standardu EMV, co zauważa się także na naszym rynku (Rys. 2, Rys. 3).



Rys. 3. Procentowy udział kart płatniczych na rynku polskim (stan na 30.06.2010)

Karty z mikroprocesorem EMV mogą być wyposażone w nowe funkcje, także z wykorzystaniem zdalnych kanałów internetowych. W mikroprocesor wbudowana jest aplikacja pozwalająca uzyskiwać jednorazowe kody do potwierdzania transakcji. Kody generuje specjalny czytnik, do którego wkłada się własną kartę i potwierdza kodem PIN. Kiszonkowe przenośne czytniki kart spełniające standard EMV stanowią najbardziej obiecujące rozwiązanie w zakresie zdalnego uwierzytelniania transakcji. Czytnik wielkości telefonu komórkowego, klient może dostać od banku. Nowe rozwiązanie wykorzystujące identyfikację dwukrokową (hasło i „wymuszona odpowiedź zwrotna" do zastosowania jednorazowego) stanowi barierę bezpieczeństwa, zwłaszcza w sytuacji nasilających się ataków typu *phishing* [15].

3.1.2. Bezpieczeństwo w bankomatach

Proces autoryzacji w bankomatach jest zależny od rodzaju bankomatu, a dokładniej od trybu komunikowania się bankomatu z główną bazą danych banku [16]:

- Stand alone – bankomaty bez podłączenia do informatycznego systemu bankowego. Komputer zainstalowany w bankomacie samodzielnie wykonuje wszystkie operacje związane z obsługą kart. W programie obsługującym bankomat zawarte są wówczas m.in. procedury obliczania PIN, dane potrzebne do tych obliczeń, wykaz numerów kart zastrzeżonych. Jest to rozwiązanie ryzykowne z uwagi na trudności z zabezpieczeniem poufności procedury obliczania PIN, braku bezpośredniej łączności z rachunkiem klienta i niską efektywność aktualizacji wykazu kart zastrzeżonych.
- Pracujące poza siecią (off-line) – bankomaty posiadają komputer nie połączony z żadnym systemem informatycznym banku, który może korzystać tylko z danych zawartych we własnej pamięci. Dane z banków przesyłane są okresowo. Stąd też nie jest możliwe dokonywanie żadnej zaawansowanej operacji, ponieważ komputer nie ma możliwości uzyskania odpowiednich informacji. Są bardziej podatne na przekłamania i nadużycia. Główną zaletą tego systemu jest jego niski koszt.
- Pracujące w trybie sieciowym (on-line) – bankomaty łączy się w sieci połączone z systemami zarządzania bankomatami, a przez ten system z systemami informatycz-

nymi banków. W systemie banku następuje sprawdzenie kwoty do wypłaty ze stanem rachunku. Dzięki możliwości autoryzacji bankomaty działające w sieci są odporne na karty sfałszowane lub bez pokrycia.

Dokonywanie transakcji w bankomacie przebiega zawsze według podobnego schematu. Po włożeniu karty konieczne jest podanie kodu PIN oraz kwoty, którą chcemy wypłacić. Następnie urządzenie dokonuje autoryzacji transakcji i w przypadku pomyślnego zakończenia tego procesu przeprowadza żądaną transakcję.

3.2. Metody kontroli dostępu do bankowości internetowej

Obecnie wszystkie Polskie banki stosują dwustopniowy poziom zabezpieczeń – jeden do logowania do rachunku, drugi do potwierdzania transakcji. Dla bezpieczeństwa banki stosują kombinacje różnych metod uwierzytelniania.

W przypadku logowania do systemu najczęściej wystarczy login i hasło (często w wersji maskowanej). Dla klienta najważniejsze jest jednak bezpieczeństwo operacji aktywnych czyli przelewów na rachunki w innych bankach.

Do metod uwierzytelniania użytkowników w systemach bankowości elektronicznej należą [9]:

1. Hasła:
   - Hasło statyczne - ustalony przez klienta ciąg znaków podawany w trakcie logowania.
   - Hasło maskowane - metoda polegająca na wprowadzaniu wybranych znaków z hasła statycznego. System za każdym razem losowo wybiera, o które znaki zapyta.
2. Karty zdrapki:
   - Lista haseł wydrukowanych na karcie w kolejności wprowadzania.
   - Karty typu „szachownica“ / „macierz“, gdzie kod buduje się z wartości umieszczonych pod konkretnymi polami np. B4F7.
3. SMS:
   - SMS z hasłem jednorazowym - na wskazany wcześniej numer telefonu przychodzi wiadomość SMS z hasłem jednorazowym.
   - SMS z opisem transakcji i hasłem jednorazowym powiązanym z tą transakcją - po wprowadzeniu danych np. do przelewu, bank wysyła do użytkownika wiadomość SMS zawierającą informacje o właśnie dokonanej czynności oraz hasło służące do potwierdzenia tej transakcji. Klient przepisuje hasło z SMSa i w ten sposób akceptuje transakcję.
4. Tokeny - urządzenia generujące hasła jednorazowe. Klient wykorzystuje je w procesie logowania lub/i do potwierdzania transakcji:
   - Token sprzętowy generujący hasła na bazie czasu - generowane hasło jest ograniczone czasowo tj. klient ma na przykład 5 minut by je wykorzystać. Po tym czasie hasło traci ważność.
   - Token sprzętowy z PINem generujący hasła na bazie licznika - token posiadający klawiaturę służącą do wprowadzenia PINu. Hasła generowane są z wykorzystaniem licznika (nie są ograniczone czasowo).
   - Token sprzętowy z PINem generujący hasła w trybie Challenge-Response - token z klawiaturą służącą do podania PINu, a także do wprowadzenia kodu transakcji (tzw. challenge), który wyświetla się po akceptacji danych np. do przelewu. Po

wprowadzeniu tego kodu urządzenie generuje odpowiedź tj. kod potwierdzający (tzw. response), który klient wpisuje pod transakcją.

- Token w telefonie generujący hasła na bazie licznika (token zabezpieczony PINem) - Metoda polegająca na generowaniu haseł jednorazowych z wykorzystaniem aplikacji instalowanej na telefonie komórkowym. Hasło generowane jest na bazie licznika. Aplikacja zachowuje się dokładnie jak token sprzętowy.
- Token w telefonie z funkcją Challenge-Response (token zabezpieczony PINem) - ta sama aplikacja, która potrafi generować hasła jednorazowe odpowiada również za potwierdzanie transakcji. W momencie, gdy klient wprowadza dane np. do przelewu i zatwierdza je, system bankowy generuje kod transakcji (tzw. *challenge*), kod ten wpisuje do aplikacji. Następnie aplikacja na telefonie wyświetla mu dane z tej transakcji (dane zostały przesłane w kodzie challenge, całkowicie w trybie *offline*) i klient musi je zatwierdzić. Po ich akceptacji aplikacja generuje kod potwierdzający (tzw. *response*), który to kod klient wpisuje pod przelewem. Jeżeli kod się zgadza transakcja jest realizowana.

5. Podpisy elektroniczne:
   - Podpis elektroniczny programowy tj. z certyfikatem i kluczami przechowywanymi na komputerze klienta (lub na dowolnym nośniku) - Klient banku podczas pierwszego logowania inicjuje na swoim komputerze generację kluczy służących do podpisu oraz uzyskuje certyfikat, który zostaje zapisany w systemie. Podczas dokonywania transakcji klient podaje hasło statyczne, które odblokowuje klucz, którym dane są podpisywane. Następnie podpisana informacja trafia do systemu bankowego.
   - Podpis elektroniczny sprzętowy - klient dostaje od banku zestaw do składania podpisu tj. czytnik, kartę z certyfikatem oraz odpowiednią bibliotekę do obsługi zestawu. Może być to również urządzenie typu USB łączące w sobie czytnik z kartą. Istnieje możliwość by klient korzystał z zestawu do podpisu kwalifikowanego. W momencie dokonywania transakcji użytkownik zostaje poproszony o podanie PINu do karty, która zawiera stosowne klucze służące do podpisania informacji.

4. Zastosowanie metod biometrycznych w celu weryfikacji tożsamości

Kolejną grupę coraz chętniej stosowanych metod kontroli dostępu stanowią systemy biometryczne. Są one zautomatyzowanymi metodami weryfikacji i rozpoznawania tożsamości ludzi.

Biometria z akademickiego punktu widzenia jest „nauką zajmującą się identyfikowaniem lub weryfikacją tożsamości osoby na podstawie jej cech fizjologicznych lub behawioralnych" [17]. Nauka ta łączy ze sobą takie dziedziny jak biologia, matematyka, statystyka, antropologia czy fizyka.

Techniki biometryczne zajmują najwyższe miejsce pod względem bezpieczeństwa, ponieważ:

- nie można ich ukraść ani pożyczyć,
- przynależą tylko do jednej osoby,
- nie można jej zapomnieć, odgadnąć, dzielić się z kimś.

Metody biometryczne badają [18]:

- *cechy fizyczne* - tęczówka oka, siatkówka (dno oka), linie papilarne, układ naczyń krwionośnych na dłoni lub przegubie ręki, kształt dłoni, kształt linii zgięcia wnętrza dłoni, kształt ucha, twarz, rozkład temperatur na twarzy, kształt i rozmieszczenie zębów, zapach, DNA itp.,
- *cechy behawioralne* - związane z zachowaniem np. sposób chodzenia, podpis odręczny, sposób pisania na klawiaturze komputera, głos.

Tab. 1. Porównanie rodzajów pomiarów biometrycznych najczęściej stosowanych w bankowości [19]

Metoda pomiaru	**Metoda biometryczna**	**Bezpieczeństwo pomiaru**	**Dokładność pomiaru**	**Koszt wdrożenia**	**Szybkość pomiaru**	**Rozmiar urządzenia**
Naczynia krwionośne palca	Światło bliskie podczerwieni	Wysokie	Wysoka	Niski	Szybki	Małe
Naczynia krwionośne ręki	Skan	Średnie	Wysoka	Średni	Średni	Średnie
Linie papilarne	Odciśnięcie palca	Średnie	Średni	Niski	Średni	Małe
Geometria twarzy	Odległości punktów charakterystycznych twarzy	Średnie	Średni	Niski	Średni	Duże
Tęczówka oka	Obraz tęczówki	Wysokie	Wysoka	Wysoki	Średni	Duże

Oprócz wymienionych wyżej charakterystyk istotne są również błędy pomiaru. Można je podzielić na dwie kategorie [17]:

- *Niesłuszna zgodność* (ang. *False Match Rate* FMR, inaczej zwane również *False Acceptance Rate* FAR), czyli częstość zatwierdzenia cechy biometrycznej w momencie kiedy tak naprawdę nie pasuje ona do modelu referencyjnego.
- *Niesłuszna niezgodność* (ang. *False Non-Match Rate* FNMR, inaczej zwane również *False Rejecion Rate* FRR), czyli częstość odrzucenia badanej cechy w momencie, gdy pasuje ona do modelu referencyjnego.

W praktyce stosuje się takie metody biometryczne, które w zależności od miejsca wykorzystania mają albo najniższe FAR, albo najniższe FRR, albo proporcjonalnie równe FAR i FRR, zwane EER (ang. *Equal Error Rate*). W praktyce zakłada się pewną wybraną wartość progową, do której porównuje się próbki. Im wyższy dobrany próg możliwego błędu, tym mniejsza omyłkowa akceptacja FAR, ale jednocześnie tym większe FRR.

Jeśli chodzi o wdrożenie systemów informatycznych w bankowości, tutaj najważniejsze jest aby wybrana metoda miała jak najniższe FAR, jednocześnie dopuszczalne jest dość duże FRR [20]. W tym szczególnym przypadku, jakim jest bank, najważniejsze jest aby wybrać taką wartość progową, która zminimalizuje popełnienie błędów niesłusznej zgodności przez system i nie wpuści przypadkowo nieuprawnionej osoby w miejsce strategiczne zabezpieczone systemem biometrycznym.

Można wyróżnić dwie metody przechowywania i transmisji wzorców biometrycznych:

- *Model z kartą (ang. match-on-card)* - Model ten zakłada użycie karty z mikroprocesorem, na której oprócz aplikacji bankowych są aplikacje zapisujące, a nawet weryfikujące dane biometryczne. W modelu tym dana biometryczna zapisana jest tylko na karcie, a nie w centralnej bazie danych banku a tym samym proces weryfikacji również odbywa się na karcie a nie w urządzeniu np. w bankomacie. Operacja wypłaty pieniędzy z bankomatu polega na pobraniu danej biometrycznej przez czytnik zainstalowany w bankomacie. Uzyskiwany skan jest szyfrowany już w momencie pobierania. Następnie pobrana, zaszyfrowana dana przesyłana jest do mikroprocesora wbudowanego w kartę kredytową, ten następnie odszyfrowuje daną i porównuje ją z daną referencyjną. Na końcu wysyła TAK lub NIE do bankomatu [21]. W wyniku tego osoba albo przeszła weryfikację i może wypłacić gotówkę, albo nie, a pobrane dane przez cały czas były bezpieczne. Model ten spełnia wymogi GIODO (Generalny Inspektor Ochrony Danych Osobowych).
- *Model bezkartowy* (ang. *match-off-card)* – w modelu tym dana biometryczna zapisywana jest w procesie rejestracji do centralnej bazy danych banku, a przy weryfikacji sprawdzana jest z modelami referencyjnymi klientów zapisanymi w tej bazie. Taki rodzaj weryfikacji jest bardzo trudny w implementacji, ponieważ wymaga bardzo szybkich łączy komunikacyjnych, a także szybkiego algorytmu porównującego dane biometryczne. W odróżnieniu do modelu z kartą, model bezkartowy może spotkać się z małą akceptacją klientów z racji braku możliwości zarządzania danymi biometrycznymi.

5. Mocne i słabe strony metod kontroli dostępu

Przy stosowaniu dowolnych zabezpieczeń podkreśla się, że łańcuch bezpieczeństwa każdego systemu jest tak silny jak najsłabsze jego ogniwo. W przypadku bankowości elektronicznej jest nim końcowy użytkownik czyli klient. Na nic się zdadzą wyszukane metody zabezpieczeń jeżeli klienci nie będą ich stosowali lub nie będą ich przestrzegali. Dużo zależy od przyzwyczajeń klientów, którzy zazwyczaj akceptują te metody, które już znają. Duże znaczenie ma również łatwość posługiwania się konkretnymi metodami.
Dla rozwoju bankowości elektronicznej ważne więc są wady i zalety metod kontroli dostępu z punktu widzenia klienta.

Tab. 2. Porównanie metod kontroli dostępu z punktu widzenia klienta

Metoda uwierzytelniania	**Bezpieczeństwo**	**Wady**	**Zalety**
Własnoręczny podpis (transakcje kartami)	Praktycznie nie zabezpiecza wcale	Łatwość podrobienia	Nie wymaga żadnego wysiłku od klienta, podpis składa się mechanicznie
PIN	Bezpieczniejszy niż podpis odręczny, ale przestępcy instalują specjalistyczne urządzenia (zarówno na bankomatach, jak i w ich wnętrzu), służące do pozyskiwania kodów PIN	Konieczność zapamiętania niekiedy dużej liczby różnych PIN-ów (do kilku kart, do logowania)	Często istnieje możliwość ustalania PIN przez klienta

Hasło (statyczne, maskowane)	Metoda nieodporna na *phishing* i większość ataków, stanowi jedynie utrudnienie (hasła z reguły są bardzo proste by nie stwarzały problemów w zapamiętaniu)	Konieczność zapamiętania hasła; dodatkowo często wymuszane przez systemy okresowe zmiany haseł.	Hasło ustala sam klient
Karta zdrapka	Narażone na *phishing* i nieodporne na ataki typu *man-in-the-middle* i *man-in-the-browser*.	Konieczność posiadania karty podczas wykonywania transakcji, konieczność zabezpieczenia karty przez zgubieniem czy kradzieżą	Nie trzeba nic zapamiętywać wystarczy posiadać kartę
SMS z hasłem jednorazowym	Zabezpiecza przed popularnymi atakami *phishingowymi*, nie zabezpiecza jednak przed atakami *man-in-the-middle* i *man-in-the-browser*.	Metoda zależna jest nie tylko od samego banku, ale również od operatora GSM	Nie trzeba nic zapamiętywać, telefon każdy nosi przy sobie
SMS z opisem transakcji	Do niedawna najbezpieczniejsza metoda na rynku. Odporna na *phishing*, ataki *man-in-the-middle* i *man-in-the browser* - o ile użytkownik czyta skrupulatnie dane trans-akcji	j.w.	j.w.
Token generujący hasła na bazie czasu	Zabezpiecza przed popularnymi atakami mającymi na celu wyłudzenie haseł do logowania /potwierdzania transakcji, ale nie zabezpiecza przed *man-in-the-middle* i *man in-the-browser*	Konieczność noszenia tokenu i posiadania go w momencie przeprowadzania transakcji	Klient nie musi niczego zapamiętywać, kody do akceptowania transakcji przepisuje się z ekranu
Token generujący hasła na bazie licznika	Jest mniej bezpieczny niż urządzenie generujące hasła ograniczone czasowo. Klient korzystający z tej metody narażony jest na wszystkie popularne ataki włącznie z *phishingiem*	j.w.	j.w.
Token generujący hasła w trybie *Challenge Response*	Poziom bezpieczeństwa większy niż w przypadku tokenów generujących hasła jednorazowe. Nie można przeprowadzić ataku *phishingowego* polegającego na wcześniejszym zdobyciu hasła. Metoda nie chroni jednak przed atakami typu *man-in-the-middle* i *man-*	j.w.	j.w.

	in-the-browser		
Podpis elektroniczny	Zabezpieczają one tylko przed *phishinigiem* i atakami *man-in-the-middle*. Są całkowicie bezbronne wobec zagrożeń typu *man-in-the-browser*	Należy posiadać nośnik kluczy do podpisu	Duża funkcjonalność podpisu elektronicznego –można go wykorzystywać do innych celów – podpisywanie dokumentów, umów itp.
Metody biometryczne	Jest to jedyna metoda, która udowadnia tożsamość osoby przeprowadzającej transakcję	Osoby mogą poczuć się dyskryminowane jeśli nie przejdą weryfikacji; obawy o bezpieczeństwo przechowywania wzorców biometrycznych	Wystarczy być, nie trzeba niczego zapamiętywać i niczego nosić

Wnioski

Technologia informacyjno-komunikacyjna umożliwiła bankom włączenie klientów do ich systemu informatycznego za pomocą zdalnych kanałów dostępu. Wirtualizacja działalności przyniosła korzyści zarówno bankom jak i klientom, ale równocześnie wymusiła rozwój różnych metod zabezpieczeń. Z uwagi na fakt, że obawy o bezpieczeństwo są jedną z głównych barier rozwoju elektronicznej bankowości, banki dokładają wszelkich starań, aby zapewnić wysoki poziom bezpieczeństwa elektronicznych transakcji. Jedną z podstawowych kategorii zabezpieczeń są metody kontroli dostępu, które zapewniają, że osoby które łączą się za bankiem i przeprowadzają transakcje są osobami do tego uprawnionymi. Polskie banki stosują cały wachlarz różnych metod kontroli dostępu – od tych najprostszych (podpisy) do tych najbardziej zaawansowanych (metody biometryczne). Należy jednak pamiętać, że klient zazwyczaj nie akceptuje metod zbyt trudnych i uciążliwych w obsłudze. Mając to na uwadze część banków umożliwia klientom wybranie metod kontroli dostępu najbardziej mu odpowiadających, aby niechęć do ich stosowania nie była barierą w korzystaniu z elektronicznej bankowości.

Literatura

1. Grzechnik J.: Bankowość Internetowa. Internetowe Centrum Promocji, Gdańsk, 2000.
2. Chmielarz W.: Systemy elektronicznej bankowości. Difin, Warszawa, 2005.
3. Kondabagil J.: Risk management in electronic banking. John Wiley & Sons Pte Ltd., Singapore, 2007.
4. Świecka B.: Detaliczna bankowość elektroniczna. CeDeWu, Warszawa, 2007.
5. Ganesan R., Vivekanandan K.: A secured hybrid architecture model for Internet Banking. Journal of Internet Banking and Commerce, Ottawa, Vol. 14, 2009, s. 1-17.
6. www.cbos.pl, 14.04.2009
7. Gospodarowicz A.: Bankowość elektroniczna, op. cit., s. 56.
8. Woda M.: Bezpieczeństwo systemów informatycznych, Politechnika Wrocławska, http://student.pwsz.elblag.pl/~stojek/bezp.sys.komp/Woda%20Marek.pdf, 24.07.09

9. Najbezpieczniejsze banki internetowe w Polsce. Raport 2009. http://www.bankier.pl/static/att/68000/2034334_raport102009.pdf; 10.11.2010
10. Gospodarowicz A.: Technologie informatyczne w bankowości. Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław, 2002.
11. Mazur Z., Mendyk-Krajewska T.: Złożoność i kompleksowość narzędzi ochrony systemów komputerowych. W: „Bezpieczeństwo systemów Informatycznych", PTI, Katowice, 2006.
12. Laskowski P.: Bezpieczeństwo elektronicznych operacji bankowych. Scientific Bulletin of Chełm, Section of Mathematics and Computer Science, No. 1/2008.
13. Tendencje i uwarunkowania rozwoju rynku kart płatniczych w Polsce, Pentor www.pentor.pl/upload_module/.../karty_platnicze.ppt; 11.11.2010
14. Zaleska M.: Współczesna bankowość. Difin, Warszawa, 2007.
15. Akademia Prawa i Informacji: Jedna karta, jeden kod. „Nowoczesny bank Spółdzielczy", 2008, nr 2, s.40-41
16. Wojciechowska-Filipek S: Technologia informacyjna w usługach bankowości elektronicznej, Difin, Warszawa, 2010.
17. Ruud M. Bolle: Biometria. Wydawnictwo Naukowo-Techniczne, Warszawa, 2008.
18. Gajewski Ł.: Biometria. http://artelis.pl/artykuly/5403/biometria;16.01.2010.
19. Taniguchi Y.: Case Study on Biometric Banking Solutions in Japan using Finger Vein Authentication Technology. Materiały z konferencji: Spring Biometric Summit 2009.
20. Ślot K.: Biometria. Politechnika Łódzka, Instytut Elektroniki, prezentacja z 20 listopada 2009 roku, http://www.eletel.p.lodz.pl/docs/ssise_2009/SSUiSE-ks.pdf, str. 82, 5 czerwca 2010.
21. Mielnicki T.: Biometria w eID, praca wykładana na konferencji Spring Biometric Summit 2009, Warszawa, http://zbp.pl/site.php?s=MTMxMzkwOTM=.

Dr Sylwia WOJCIECHOWSKA-FILIPEK
Katedra Zarządzania
Społeczna Wyższa Szkoła Przedsiębiorczości i Zarządzania
00-842 Warszawa, ul. Łucka 11
e-mail: wojciecs@wit.edu.pl