prof. dr hab. inż. Marian KOPCZEWSKI,
dr Jarosław STELMACH
Wyższa Szkoła Oficerska Wojsk Lądowych we Wrocławiu

ZABEZPIECZENIA BIOMETRYCZNE ELEMENTEM SYSTEMU BEZPIECZEŃSTWA MARYNARZY

STRESZCZENIE

W artykule przedstawiono podstawowe zagadnienia związane z możliwością wykorzystania i zastosowania danych biometrycznych. Przeprowadzone badania pozwalają na stwierdzenie, że w oczach badanych systemy biometryczne są dość znanymi systemami zabezpieczeń, które zapewniają wysoki poziom bezpieczeństwa i ułatwiają codzienne procesy. Z drugiej strony techniki te uznawane są wciąż za techniki obarczone wysokimi kosztami, prowadzącymi do nadużyć z wykorzystaniem danych. Dalej idąc, należy stwierdzić, że ich występowanie zdaniem badanych ma największy zakres w usługach finansowych i w zabezpieczaniu dokumentów tożsamości. Wyniki wykazują, iż poziom akceptacji systemów biometrycznych w rejestracji czasu pracy w organizacjach, jakimi są również okręty, przez użytkowników staje się dziś sprawą powszechną i bezsprzeczną, stają się one tym samym elementem zarządzania zasobami ludzkimi w każdej organizacji zmilitaryzowanej.

WSTĘP

Możliwości wykorzystania danych biometrycznych są coraz większe a co za tym idzie wzrasta również ich praktyczne zastosowanie. Dlatego kluczowym elementem, który należy uwzględnić w trakcie projektowania, budowy i eksploatacji systemów wykorzystujących biometrię, jest problemem przypisania właściwej osoby do właściwego dokumentu. Oczywiście zakłada się, że system spełnia wszelkie wymogi związane z ochroną swoich zasobów danych, czyli danych bardzo wrażliwych, umożliwiających identyfikację i weryfikację osób. Zakłada się, że nie pozwalają one na kradzież tożsamości czy też na stworzenie nowej/własnej tożsamości. Możliwość, a w niektórych przypadkach konieczność, zastosowania danych biometrycznych wynika z coraz szerszego

wykorzystania technologii informatycznych, w szczególności internetowych, w życiu codziennym i coraz częstszych prób kradzieży tożsamości osób korzystających z tych technologii. Współczesne systemy informatyczne bardzo często mają zapewniony wysoki poziom bezpieczeństwa w zakresie ochrony i dostępu do danych, a szczególnie zarządzania zasobami ludzkimi w każdej organizacji, a w strukturach wojska - marynarzy szczególnie.

W artykule przedstawione zostały podstawowe zagadnienia związane z możliwością wykorzystania i zastosowania danych biometrycznych, jako wartości zabezpieczeń biometrycznych w aspekcie bezpieczeństwa i kontroli pracowników – żołnierzy - marynarzy, co oznacza, że przedmiotem analizy jest postrzeganie stosowania zabezpieczeń tego typu między innymi na okrętach .

PODSTAWOWE DEFINICJE

Biometria to nauka zajmująca się ustalaniem i potwierdzeniem tożsamości na podstawie mierzalnych cech organizmu. Inaczej mówiąc, biometria jest zbiorem metod i technik służących do weryfikacji i ustalania tożsamości osób na podstawie ich cech biofizycznych i behawioralnych[1]. Za biometrię uważa się zbiór technik, służących pomiarom cech fizycznych i behawioralnych człowieka w celu automatycznego rozpoznawania danej osoby, czyli potwierdzenia lub odrzucenia jej tożsamości dla celów bezpieczeństwa[2].

Biometrię można również zdefiniować jako metodę automatycznej identyfikacji osobistej opartej na pewnych cechach fizycznych lub behawioralnych człowieka. Cechy te stanowią właśnie dane biometryczne. Największy rozwój systemów biometrycznych rozpoczął się w latach 90-tych ubiegłego wieku[3]. Wówczas rozpoczęto prowadzenie prac nad doskonaleniem, przede wszystkim w zakresie zabezpieczeń, między innymi przed możliwościami oszustw przez osoby nieuprawnione.

Termin „biometria" pochodzi od greckiego słowa bio (życie, żywy, procesy życiowe) oraz metrics (mierzyć). Biometria zajmuje się mierzeniem cech biologicznych, a jej głównym zadaniem jest automatyczne rozpoznawanie osób. Idea wykorzystywania niepowtarzalnych cech ciała do identyfikacji znana jest od setek, a nawet tysięcy lat[4]. Babilończycy używali odcisków palca w wosku jako pieczęci. Rozwój zintegrowanych systemów biometrycznych jest jednak bardzo młodą dziedziną zabezpieczeń, związaną z rozwojem technologii infor-

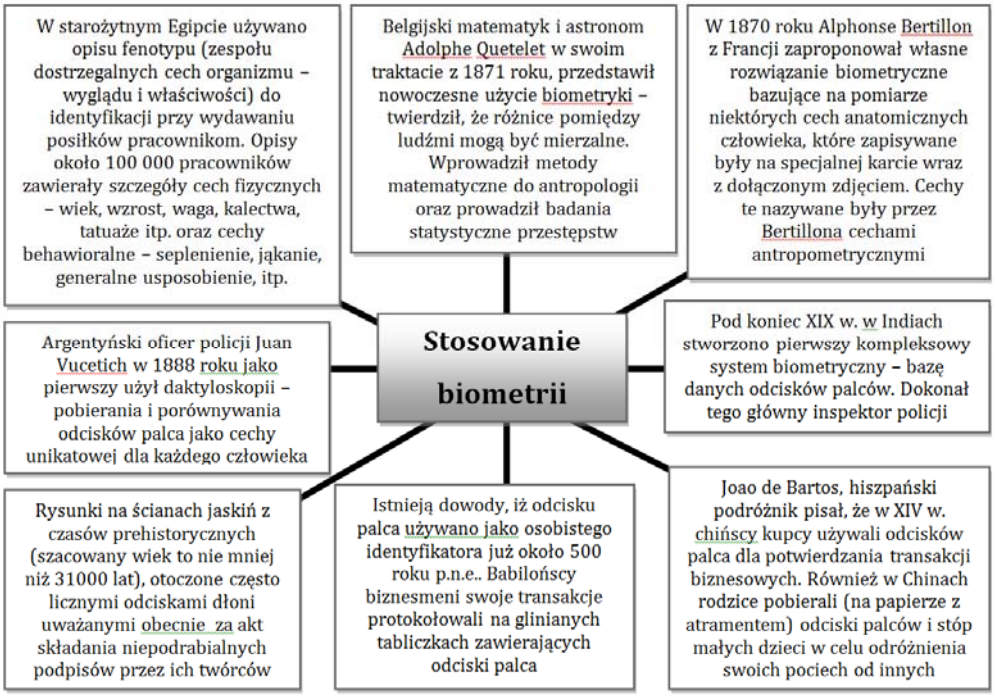
[1] M. Chałon*: Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych*. Wrocław 2007, s. 40.

[2] R. Anderson: *Inżynieria zabezpieczeń*. Warszawa 2007, s. 56.

[3] P. Niedziejko, I. Krysowaty: *Biometria. Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie* [w:] Zabezpieczenia nr 4, Warszawa 2006, s. 14.

[4] *Biometria* [w:] Patrol - Magazyn Securitas w Polsce nr 4, Warszawa 2007, s. 6.

matycznych. Ze względu na dużą dokładność i niezawodność urządzeń odczytujących dane biometryczne oraz dużą moc obliczeniową komputerów, potrafiących te dane analizować, biometria stała się popularnym sposobem ochrony dostępu do danych przed osobami nieupoważnionymi. Rysunek nr 1 przedstawia odnotowane przykłady stosowania biometrii od początku ludzkości.



Rys. 1. Stosowanie biometrii na przestrzeni dziejów ludzkości

źródło: Biometria [w:] Patrol - Magazyn Securitas w Polsce nr 4, Warszawa 2007, s. 6

Reasumując, należy stwierdzić, iż biometria jest często definiowana w jej wąskim funkcjonalnym znaczeniu, tymczasem trzeba sobie uzmysłowić, że jest to sięgająca korzeniami 31 000 lat, nauka o prawach rządzących zmiennością cech populacji organizmów, której wyniki opracowywane są za pomocą metod statystyki matematycznej. Wywodzące się z nauk biologicznych klasyczne analizy i badania biometryczne, dzięki dokonującej się rewolucji technologicznej, znalazły swoje odzwierciedlenie w funkcjonalnych aplikacjach nowoczesnych technologii informacyjnych zdolnych do udostępniania i zaawansowanego przetwarzania określonych danych biometrycznych.

ISTOTA BIOMETRII

Termin „biometria" zwiódł i zmylił wielu badaczy i amatorów. Zanim więc zostanie przedstawiona istota biometrii należy zaznaczyć, iż wbrew niektórym wyobrażeniom i przypuszczeniom biometria nie jest działem metrologii, zajmującym się pomiarami parametrów i cech rozmaitych systemów biologicznych. Takie pomiary i obserwacje są wprawdzie dokonywane na gruncie anatomii, histologii, antropologii, fizjologii, biofizyki, jednak sam proces i metodyka odpowiednich pomiarów nie odbiega w niczym klasycznym od pomiarów wykorzystywanych w technice, fizyce czy chemii.

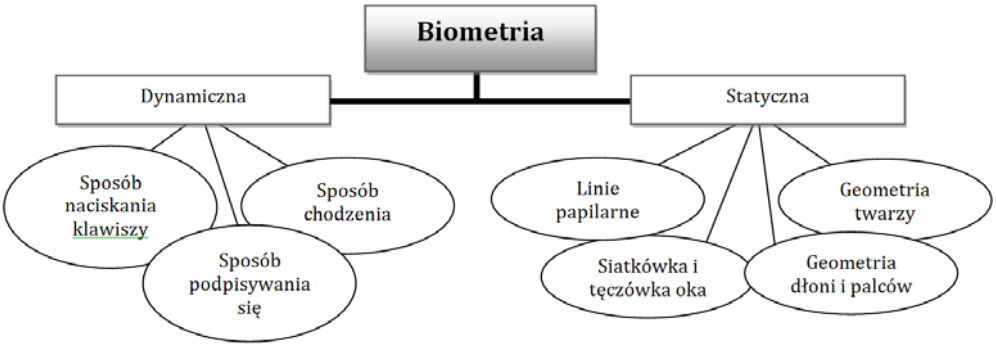
Jednak tak powielane obserwacje i pomiary, w dodatku obarczone czynnikami obniżającymi ich wiarygodność, stanowią bardzo niepewną i niewygodną podstawę przy próbach wnioskowania, na ich podstawie o właściwościach obiektów i zjawisk a także przy próbach uogólnień i praktycznych zastosowań wyników badań naukowych. Dlatego niezbędnym elementem każdego pomiaru i każdej oceny odniesionej do systemów biologicznych musi być statystyczne opracowanie wyników. Dzięki takiemu opracowaniu możliwe staje się sprowadzenie wielu mało czytelnych pomiarów do kilku łatwych w interpretacji wskaźników. W dodatku rozsądnie stosowana statystyka daje możliwości precyzyjnego wnioskowania w oparciu o niepewne i obarczone błędami dane. W ten sposób biometria jest elementem wydobywającym porządek z chaosu, czynnikiem pozwalającym przezwyciężyć podstawową sprzeczność, jaka istnieje pomiędzy naturą zindywidualizowanych osobniczo obserwacji biologicznych i wywodzącymi się z ideałów nauk ścisłych tendencji formułowania sądów ogólnych i uniwersalnych[5].

Entuzjaści biometrii uznają ją za najbezpieczniejsze i najwygodniejsze narzędzie, służące autoryzacji i identyfikacji danej osoby, przy jednoczesnym uniemożliwieniu nieautoryzowanego dostępu do informacji, tajemnic i danych. Natomiast przeciwnicy biometrii wskazują na możliwość ingerencji w prawa człowieka, a także na fakt, że w dobie nowych technologii dane biometryczne łatwo sfałszować. Ich zdaniem wątpliwości co do możliwości naruszenia praw i wolności człowieka wynikają z szerokiego wykorzystania tego typu danych oraz powszechności i braku kontroli przy ich zbieraniu i przetwarzaniu.

Rozróżniamy dwa główne aspekty biometrii, rysunek 2: statyczną – fizyczno-biologiczną, oraz dynamiczną – behawioralną. Biometria statyczna polega na rozpoznawaniu cech budowy ciała człowieka, takich jak: geometria twarzy, siatkówka i tęczówka oka, głos, geometria dłoni i palców czy linie papilarne. Z kolei biometria dynamiczna rozpoznaje takie cechy zachowania czło-

[5] R. Tadeusiewicz, A. Izworski, J. Majewski: *Biometria*. Kraków 1993, s. 8.

wieka jak: sposób chodzenia, sposób naciskania klawiszy, cechy podpisu lub sposób podpisywania się.



Rys. 2. Podstawowe aspekty biometrii

źródło: M. Chałon: Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych, Wrocław 2007, s. 40

W dzisiejszych czasach biometria stanowi zestaw kompleksowych metod, które w znacznej części są przeznaczone do szczegółowej identyfikacji bądź weryfikacji tożsamości ludzi. Proces ten odbywa się za pomocą wielosegmentowej analizy zróżnicowanych i niepowtarzalnych cech fizycznych lub behawioralnych. Warto w tym momencie wyjaśnić istotę pojęć weryfikacji i identyfikacji. Weryfikacja, polega na szczegółowym sprawdzeniu, czy osoba identyfikująca się z daną tożsamością jest rzeczywiście tą, z którą się identyfikuje. Proces weryfikacji stanowi tym samym zadanie możliwe do realizacji za pomocą relatywnie mało wydajnych systemów informatycznych. Na całość procesu składa się porównanie zarejestrowanej przez specjalne urządzenie tzw. czytnik, mikrofon lub kamerę, próbki z przechowywanym w bazie danych wzorcem. Natomiast jeśli chodzi identyfikację, to proces bardziej złożony, często bowiem zdarza się, że identyfikacja danej osoby przeprowadzana jest w oparciu o bardzo duży zakres danych. Dane zebrane przez czytnik trzeba wtedy porównać z bazą milionów osób. Identyfikacja jest stosowana głównie przez instytucje rządowe, służby policyjne, sądownictwo oraz wojsko.

W praktyce, stosowane są zróżnicowane metody i techniki identyfikacji bądź weryfikacji osób. Wszystkie one jednak znacząco zróżnicowane są przede wszystkim pod względem skuteczności, kosztów i tzw. inwazyjności. Inwazyjność stanowi tu jednak element obarczony istotnym subiektywizmem, w przypadku identyfikacji i weryfikacji odnosi się raczej do naruszenia godności i przestrzeni osobistej, aniżeli do wtargnięcia specjalnych urządzeń pomiarowych do organizmu człowieka.

PRAWNE ASPEKTY BIOMETRII

Stosowanie metod i technik biometrycznej weryfikacji i identyfikacji w zakresie wielu dziedzin życia i gospodarki staje się powszechne. Jednakże pomimo, iż wykorzystywane w codziennej praktyce osiągnięcia biometryczne ulegają ciągłemu rozwojowi, to jednak nie wszystkie aspekty ich stosowania są jednoznacznie ustalone. Bardzo znaczącym, jawi się aspekt spełnienia najwyższych poziomów bezpieczeństwa danych prywatnych jak i wysokiego standardu jakości ich pobierania i przechowywania. Specjaliści z zakresu biometrii wskazują, iż priorytet stanowi tu bezpieczeństwo indywidualnie zebranych cech tożsamości w rozwiniętym systemie teleinformacyjnym, w ramach którego obserwowane jest powszechne korzystanie z usług elektronicznych, odbywających się za pośrednictwem coraz bardziej nowoczesnych urządzeń. Należy zwrócić szczególną uwagę by za rozwojem technologii nadążało rozumienie i interpretacja prawa. Jest to o tyle istotne gdyż przy wykorzystaniu biometrii jako nowej technologii do identyfikacji i uwierzytelnienia osób toczą się wielkie dyskusje w ramach, ochrony danych osobowych i zrozumienia niektórych prawnych aspektów wykorzystania biometrii.

Zgodnie z Ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (skrót: UODO) dane osobowe to „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej”[6]. Ze względu na to, iż dane biometryczne co do zasady spełniają przesłanki przewidziane w definicji legalnej danych osobowych, ich status prawny w większości przypadków uregulowany będzie przez wspomnianą wyżej ustawę oraz ustawy szczególne[7].

Same dane biometryczne nie są zdefiniowane wprost w UODO, jeśli jednak odpowiadają one przesłance określonej w art.6 UODO (dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, z uwzględnieniem ust. 2 i 3 art. 6), będą chronione na podstawie tego aktu prawnego. Brak legalnej definicji w UODO nie oznacza, że w polskim lub w unijnym ustawodawstwie takich definicji nie ma. Pojęcie danych biometrycznych pojawia się w ustawie o dokumentach paszportowych[8]. Zdefiniowane zostało w niej, jako wizerunek twarzy i odciski palców umieszczone w dokumentach paszportowych w formie elektronicznej (art. 2 pkt. 1). Sporządzeniem dokumentu paszportowego zgodnie z tą ustawą, jest przeniesienie danych osobowych i biometrycznych osoby ubiegającej się o wydanie dokumentu paszportowego do książeczki paszporto-

[6] Dz. U. z 1997 r. Nr 133, poz. 883 ze zm.
[7] R. W. Kaszubski: *Biometria w bankowości i administracji publicznej*. Warszawa 2010, s. 6.
[8] Dz. U. z 2006 r. Nr 143, poz. 1027 ze zm.

wej w postaci graficznej i elektronicznej (art. 2 pkt.4). wydaje się, że definicja przedstawiona w ustawie o dokumentach paszportowych jest dość wąska, gdyż w literaturze do danych osobowych zalicza się również DNA, obraz tęczówki oka, itp[9].

W prawie unijnym kwestie związane z danymi biometrycznymi reguluje rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży, wydawanych przez Państwa Członkowskie, w którym za dane biometryczne uznaje się wyraz twarzy oraz odcisk palców (art. 2 ust. 2) [10].

Sama ustawa o ochronie danych osobowych wskazuje wśród grupy danych wrażliwych, m.in. dane o kodzie genetycznym, co oznacza, że dane biometryczne w większości przypadków będą traktowane jako dane wrażliwe, w związku z czym będą się do nich odnosić wszystkie zasady dotyczące danych wrażliwych. Przy ich przetwarzaniu będzie więc stosowany albo co najmniej podwyższony poziom zabezpieczenia danych (jeśli żaden z komputerów przetwarzających dane biometryczne nie będzie podłączony do sieci publicznej), albo wysoki poziom zabezpieczenia danych biometrycznych (jeśli co najmniej jeden komputer będzie podłączony do sieci publicznej).

W odniesieniu do zbierania danych biometrycznych w postaci odcisków palców i umieszczania ich w bazie danych, w celu identyfikacji dostępu i ewidencji czasu pracy w przedsiębiorstwie wydaje się być stosowne w odniesieniu do literatury prawa w ramach dwóch przypadków[11]:

- Pracodawca będzie wykorzystywał dane biometryczne w systemach rejestracji czasu pracy, jednakże dane biometryczne będą przechowywane bezpiecznie tylko na karcie bezstykowej i porównywane przez bezpieczny czytnik biometryczny, a nie oprogramowanie centralne. Pracownik zgadza się na takie rozwiązanie,
- Pracodawca będzie wykorzystywał biometrię tylko do kontroli dostępu do pomieszczeń w budynkach firmy (dane na serwerze).

Zasadnicze znaczenie w zakresie stosowania technologii biometrycznych w przedsiębiorstwach ma odniesienie uodo do uregulowań Kodeksu pracy oraz związana z tym możliwość i legalność wyrażenia zgody na pobieranie i gromadzenie danych biometrycznych.

Jeżeli pominąć właściwości techniczne poszczególnych rodzajów biometrii, tzn. traktować jednolicie system centralny i system karty oraz dane i wzorce danych, to Kodeks pracy zawiera jasno zdefiniowane wymogi dla ja-

[9] A. Adamski i in.: *Internet. Ochrona wolności, własności i bezpieczeństwa.* Warszawa 2011, s. 246-248.

[10] Dz. Urz. z 29 grudnia 2004 r., UE L 385.

[11] R. W. Kaszubski: *Biometria w bankowości i administracji publicznej*. Warszawa 2010, s. 9.

kiegokolwiek zbierania danych biometrycznych[12]. Jednakże należy pamiętać, iż Kodeks pracy sankcjonuje jednoznacznie, ze dobrowolne umieszczenie danych biometrycznych w postaci wzorca biometrycznego na karcie oznacza, iż dysponentem danych jest ich posiadacz. W tym przypadku pracodawca nie może wykorzystywać tego rodzaju danych, a ewentualna próba pozyskania ich wiąże się z nieproporcjonalnie dużymi środkami i nakładami. Dlatego też przy stworzeniu tak bezpiecznego systemu można poddać w wątpliwość spełnienie przez tak zabezpieczone wzorce biometryczne, przesłanek, koniecznych dla danych osobowych.

Warto zaznaczyć w tym miejscu, iż prawa i obowiązki pracownika i pracodawcy mają, co do zasady, charakter względny. Dzieje się tak, bowiem, iż normy Kodeksu pracy w odniesieniu do regulaminu pracy dają duże możliwości stosowania rozwiązań biometrycznych do pomiaru czasu pracy lub dostępu do pomieszczeń służbowych. W kodeksie pracy jest jasno zapisane, iż w szczególnych przypadkach regulamin pracy może ustalać „organizację pracy, warunki przebywania na terenie zakładu pracy" oraz „przyjęty u danego pracodawcy sposób potwierdzania przez pracowników przybycia i obecności w pracy". Jako, że „pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów" i art. 104 wprowadza pod pewnymi warunkami obowiązek istnienia regulaminu pracy, wyrażenie zgody na biometryczny pomiar czasu pracy lub dostęp do pomieszczeń służbowych, mogłoby być zalegalizowane poprzez przepisy regulaminu pracy[13].

SYSTEMY BIOMETRYCZNE I ICH DZIAŁANIE

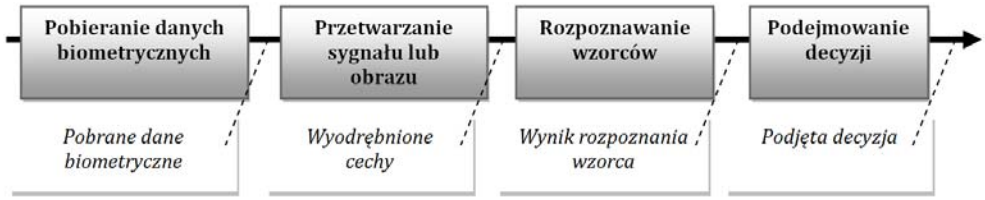
Praktyka pokazuje, że w większości systemów najbardziej zawodnym elementem bywa człowiek, toteż doskonalenie istniejących systemów oraz konstruowanie nowych, ma m.in. na celu, jeśli nie wyeliminowanie tego czynnika, to przynajmniej jego minimalizację. Badania pokazują również, ze systemy wykorzystujące biometrię dają większą gwarancję właściwego określenia tożsamości użytkownika systemu (w przeciwieństwie do systemów, które korzystają z jego wiedzy). Systemy wykorzystujące biometrię, dają kilka zasadniczych korzyści, których nie posiadają systemy zbudowane w oparciu o inne metody. Podstawowa różnica pomiędzy tymi systemami polega na tym, że danych biometrycznych nie można pożyczyć, ukraść, ani zapomnieć.

[12] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych. Komentarz*. Kraków 2007, s. 342.

[13] R. W. Kaszubski*: Biometria w bankowości i administracji publicznej*. Warszawa 2010, s. 9.

Systemy biometryczne kojarzą się przede wszystkim z pobieraniem odcisków linii papilarnych palców lub skanowaniem tęczówki oka. Tymczasem wciąż poszukuje się coraz to nowych cech fizycznych i behawioralnych człowieka, unikalnych tylko dla niego, a zatem odróżniających go od każdej innej osoby. Niektóre z nich dostępne są już w formie gotowych rozwiązań na rynku, inne znajdują się w fazie badań i testów.

Istotnym elementem zwiększającym szansę na zaprojektowanie i wdrożenie systemu biometrycznego, jest akceptacja pomiaru i sposobu „pobierania" danej cechy biometrycznej. Moduły rejestracji i identyfikacji współpracują ze sobą oraz realizują zadania związane z pobraniem surowych danych biometrycznych, ekstrakcją cech, porównaniem zestawów cech oraz podejmowaniem decyzji. Rysunek 3 przedstawia schemat postępowania podczas przetwarzania danych biometrycznych.



Rys. 3. Etapy przetwarzania danych biometrycznych

źródło: J. Barta, P. Fajgielski, R. Markiewicz: Ochrona danych osobowych. Komentarz, *Kraków 2007, s. 342*

Klasycznym przykładem jest tutaj pobieranie odcisków linii papilarnych, co jest jednoznacznie kojarzone z popełnieniem przestępstwa i koniecznością pobrania tych linii przez policję. Drugą stronę zagadnienia stanowią urządzenia i sposoby kontroli biometrii, wszelkiego rodzaju czytniki i bramki kontrolne. Powinny one być łatwe i szybkie w użyciu, precyzyjnie działające (poziom błędów w odrzuceniach i akceptacji), odporne na próby zakłóceń oraz oczywiście niezbyt kosztowne na etapie zakupu i eksploatacji. W przypadku urządzeń, które miałyby służyć do zdalnej lub lokalnej autoryzacji, konieczne może się okazać rozpoznanie nie tylko osoby, ale także jej woli. Może to powodować, że urządzenia będą musiały mieć możliwość rozpoznawania akcji, służących jako odzwierciedlenie woli danej osoby. Można w takich przypadkach wykorzystać, np. podpis tej osoby - specyficzne ruchy dłoni, ruchy oka lub innych części ciała a także wypowiedziane słowo lub zdanie.

Aktualnie na rynku urządzeń biometrycznych dostępna jest szeroka oferta tego typu systemów. Najpopularniejsze z nich to urządzenia w postaci czytników linii papilarnych stosowanych przeważnie do systemów kontroli dostępu oraz tzw. terminale bazujące na weryfikacji odcisku palca w formie

cyfrowej, które ponadto działają w formie systemu dualnego, umożliwiającego dwa rodzaje autoryzacji poprzez linie papilarne i karty zbliżeniowe. Praca systemów biometrycznych, realizujących funkcje weryfikacji opiera się na potwierdzeniu tożsamości osoby, która poddaje się temu procesowi. Praktycznie oznacza to rozpoczęcie uwierzytelniania poprzez dokonanie właściwej preselekcji weryfikowalnych danych, np. za pomocą podania danych biometrycznych zapisanych na nośniku, jakim może być karta. Odpowiedni wektor cech biometrycznych zostaje porównany ze swoim odpowiednikiem w systemie i podejmowana jest decyzja o ich zgodności lub ich braku. Ten tryb nazywany jest trybem 1:1. Rozwiązanie takie pozwala dokonywać weryfikacji w systemach o zdecydowanie mniejszych wymaganiach wydajnościowych, wymaga również krótszego czasu na realizację tej funkcji.

Systemy realizujące przede wszystkim, funkcje identyfikacji ukierunkowane są na jednoznaczne określenie tożsamości danego użytkownika. Niepotwierdzaną przynależności określonych cech biometrycznych dla danej osoby; ale biorąc pod uwagę jej cechy biometryczne, potrafią jednoznacznie ją zidentyfikować. Po odczytaniu zadanych cech biometrycznych i odpowiednim przekształceniu ich do postaci cyfrowej, dokonują przeszukania dostępnych zasobów danych, w celu znalezienia obiektu najbardziej zbliżonego do badanego. Jest to podstawą do ustalenia tożsamości badanej osoby. Biorąc pod uwagę sposób działania tych funkcji, identyfikacja określana jest jako tryb 1:N (jeden do wielu). Stwierdzenie „najbardziej zbliżonego do badanego" mówi, że pozytywna odpowiedź jest możliwa po osiągnięciu określonego progu zgodności szukanego zestawu cech biometrycznych ze znalezionym.

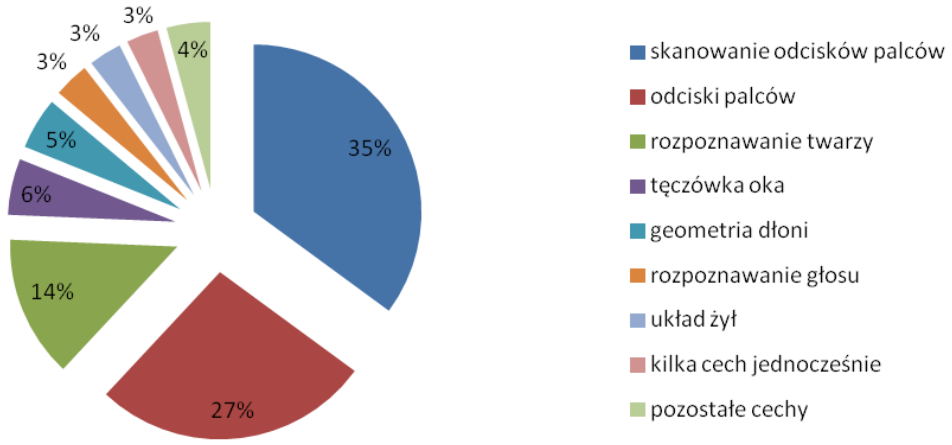
Działanie systemów biometrycznych powinno uniemożliwiać powtórne zarejestrowanie użytkownika w bazie danych. Innymi słowy system nie powinien umożliwiać zarejestrowania tej samej tożsamości z innymi danymi identyfikacyjnymi. Jest to szczególnie istotne w systemach wymagających wysokiego bezpieczeństwa. Zmiana danych osobowych nie ma wpływu na wynik identyfikacji, a osoba raz wprowadzona do bazy danych (jako określony zestaw danych biometrycznych) jest zawsze identyfikowana pod pierwotnie wprowadzonymi danymi. Wynikiem takiego podejścia jest efektywne zabezpieczenie przed próbami ukrywania lub zmiany tożsamości.

WYKORZYSTYWANIE TECHNOLOGII BIOMETRYCZNEJ

Do cech fizycznych, które mogą być wykorzystane w systemach biometrycznych można zaliczyć: barwę głosu, zapach, linie papilarne palców (odcisk palca i odcisk opuszka palca), naczynia krwionośne palców, geometrię dłoni, geometrię i rysy twarzy, rozkład temperatury twarzy, analizę faktury powierzchni twarzy - skóry, geometrię ucha, geometrię ust, cechy charaktery-

styczne tęczówki oka, cechy charakterystyczne siatkówki oka, układ żył nadgarstka, strukturę włosów, paznokci, EEG, ECG, identyfikację DNA. Biorąc pod uwagę cechy behawioralne, można wymienić charakterystykę: głosu, mowy, ruchu ust, ruchu gałki ocznej. Wyróżnić można także: pismo (podpis odręczny), sposób pisania na klawiaturze, charakterystykę chodu[14].

Niektóre z przedstawionych powyżej cech są już wykorzystywane, niektóre są na etapie badań i prób wdrażania. Nie wszystkie z tych cech znajdują praktyczne zastosowanie. Pojawiają się również nowe propozycje, które spełniają opisane poniżej właściwości i mogą być w przyszłości wykorzystane jako cechy biometryczne. Zalicza się do nich: kształt całego ciała człowieka, analiza wibracji twarzy lub głowy w czasie mówienia, badanie wewnętrznej struktury ciała i jego funkcji życiowych, analiza pól magnetycznych lub elektrycznych generowanych przez ciało człowieka lub reakcji na takie pola. Praktyczne wykorzystanie poszczególnych cech biometrycznych przedstawia rysunek 4.



Rys. 4. Praktyczne wykorzystanie technologii biometrycznych

źródło: I. Iskierka, S. Iskierka: Przegląd podstawowych technologii biometrycznych, Częstochowa 2010, s. 116

[14] A. Wiśniewski: *Metody oceny systemów rozpoznawania mówców*, Biuletyn IAiR WAT 2000, Nr 13, s. 22.

Natomiast główne obszary zastosowań można sklasyfikować następująco[15]:

- sprawiedliwość i obronność: identyfikacja zwłok, śledztwa kryminalne, identyfikacja terrorystów, poszukiwania zaginionych, instytucje wojskowe i specjalne, instytucje strategiczne- banki, elektrownie, rafinerie;
- administracja publiczna: dowody osobiste, prawa jazdy, podpis cyfrowy, świadczenia społeczne, kontrola paszportowa, kontrola graniczna;
- zastosowanie komercyjne: praca przy komputerze, ochrona danych, e-handel, dostęp do Internetu, karty kredytowe i płatnicze, fizyczna kontrola dostępu, telefony komórkowe, zarządzanie dokumentacją medyczną zdalne nauczanie, zarządzanie czasem pracy, dostęp do bibliotek i publicznych zasobów danych, masowe imprezy.

Analizując zabezpieczenia za pomocą danych biometrycznych, należy stwierdzić, iż mają one bardzo duże perspektywy wykorzystania w przyszłości. I właśnie to co odróżnia dane biometryczne od pozostałych form służących do identyfikacji i weryfikacji, a więc niemożność ich zgubienia, zapomnienia i podrobienia, jak ma to miejsce w przypadku jakichkolwiek haseł, kluczy, itp., nadaje im wartość ponadczasowego zabezpieczenia. Jednakże poza niekwestionowaną przydatnością technologii biometrycznych w różnego rodzaju zabezpieczeniach rodzi się zasadnicze pytanie, która forma z aktualnie dostępnych jest najlepsza.

PRZYGOTOWANIE I BEZPIECZEŃSTWO DANYCH

Zakładając, że bezpieczeństwo danych identyfikacyjnych w systemach informatycznych jest na odpowiednio wysokim poziomie, podstawowym problemem, z którym mamy do czynienia jest kwestia przypisania osoby do dokumentu, który jest wykorzystywany do identyfikacji tej osoby. W tym właśnie celu wykorzystuje się dane biometryczne, które są umieszczane w dokumencie identyfikacyjnym. Dane te mogą być dwojakiego rodzaju. Z jednej strony są to dane, które można zweryfikować bezpośrednio- bez korzystania ze specjalistycznych sprzętów, np. zdjęcie biometryczne; z drugiej strony są to dane zapisane w części elektronicznej dokumentu- w mikroprocesorze które można zweryfikować tylko i wyłącznie przy pomocy specjalistycznych urządzeń, czyli np. czytników lilii papilarnych.

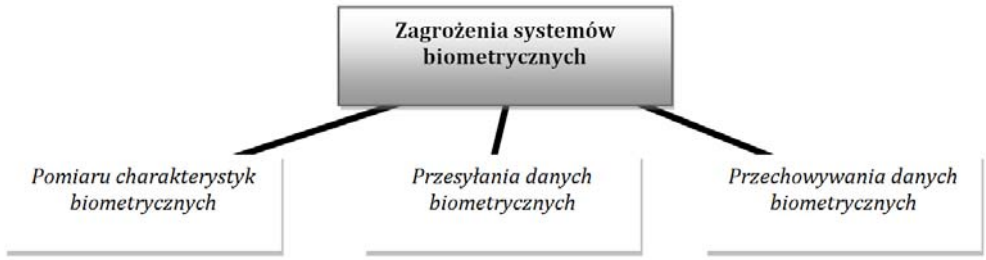
Analiza podstawowych technologii biometrycznych wykazuje jednoznacznie, iż każdy system biometryczny narażony jest na inne zagrożenia.

[15] R. W. Kaszubski: *Biometria w bankowości i administracji publicznej*. Warszawa 2010, s. 11.

W związku z tym każdy system wymaga innej ochrony. Warto nadmienić, że kanały komunikacyjne w zakresie poszczególnych technologii biometrycznych są istotną częścią całego systemu. Dlatego też istotnym jest zapewnienie im niemniejszego zabezpieczenia. Jest to o tyle istotne, gdyż zabezpieczenie kanałów komunikacyjnych przebiegających wewnątrz jednego urządzenia analizującego dane biometryczne, stanowi w procesie niezmiernie łatwiejszy krok, co więcej może on być zastosowany do zabezpieczenia całości systemu.

Jakiekolwiek próby złamania systemu biometrycznego mogą skupiać się na szerokim zakresie różnych ogniw całego systemu biometrycznego. Znacząca liczba ataków i prób złamań systemu jest wielce podobna do ataków na dowolnie dobrane systemy informatyczne. Za przykład można tu przywołać sytuację próby ataku na etapie przetwarzania danych, oznaczającą zamianę głównych algorytmów systemu. Może to być dokonane poprzez bezpośrednią ingerencję w sprzęt, bądź też w oprogramowanie. Ważne pozostają tu więc zasady ochrony fizycznej oraz przeciwwłamaniowej i przeciwwirusowej znane z innych działów budowy systemów informatycznych. Dla wszystkich zresztą elementów biometrycznego systemu bezpieczeństwa należy stosować dobre praktyki obowiązujące przy konstruowaniu dowolnych, bezpiecznych systemów informatycznych[16].

Spectrum występowania zagrożeń dotyczących systemów biometrycznych, ze względu na ich specyfikę, jest jednak nieco szersze niż w przypadku standardowych systemów informatycznych. Rysunek 5 przedstawia podstawowe typy zagrożeń systemów biometrycznych.



Rys. 5. Podstawowe zagrożenia systemów biometrycznych

źródło: Ł. Stasiak, A. Czajka, P. Strzelczyk, M. Chochowski, A. Pacut: Od biometrii do bezpiecznej biometrii, Warszawa 2007, s. 5

Istotnym jest tu także fakt, że tak samo jak ma to miejsce w ramach innych systemów zabezpieczeń, użytkownik systemu zabezpieczeń biometrycznych jest jego integralną częścią. W związku z tym by to ogniwo nie stało się najsłabszym ogniwem, użytkownik musi zawsze zostać odpowiednio przeszko-

[16] D. Denning: *Wojna informacyjna i bezpieczeństwo informacji*. Warszawa 2002, s. 43

lony w zakresie korzystania z danego systemu i możliwych nadużyć. Bowiem wiadomym jest, iż całość systemu jest na tyle stabilna i silna jak jego najsłabsze ogniwo.

WNIOSKI

Reasumując rozważania teoretyczne odnośnie biometrii wysuwa się jeden wniosek, iż jest to jedno z najbezpieczniejszych i najwygodniejszych narzędzi, służące autoryzacji i identyfikacji osób, przy jednoczesnym uniemożliwieniu nieautoryzowanego dostępu do informacji, tajemnic, danych, które są dziś niezbędne dla żołnierzy, a marynarzy szczególnie. Systemy biometryczne kojarzą się przede wszystkim z pobieraniem odcisków linii papilarnych palców lub skanowaniem tęczówki oka. Tymczasem wciąż poszukuje się coraz to nowych cech fizycznych i behawioralnych człowieka, unikalnych tylko dla niego, a zatem odróżniających go od każdej innej osoby. Niektóre z nich dostępne są już w formie gotowych rozwiązań na rynku, inne znajdują się w fazie badań i testów. Analizując zabezpieczenia za pomocą danych biometrycznych, należy stwierdzić, iż mają one bardzo duże perspektywy wykorzystania w przyszłości. I właśnie to, co odróżnia dane biometryczne od pozostałych form służących do identyfikacji i weryfikacji, a więc niemożność ich zgubienia, zapomnienia i podrobienia, jak ma to miejsce w przypadku jakichkolwiek haseł, kluczy, itp., nadaje im wartość ponadczasowego zabezpieczenia. Zatem biometria staje się elementem zarządzania zasobami ludzkimi w każdej organizacji zmilitaryzowanej, w tym jednostkach marynarki wojennej,

BIBLIOGRAFIA

[1] Adamski A. i in.: *Internet. Ochrona wolności, własności i bezpieczeństwa.* Warszawa 2011.

[2] Anderson R.: *Inżynieria zabezpieczeń*. Warszawa 2007.

[3] Barta J., Fajgielski P., Markiewicz R.: *Ochrona danych osobowych. Komentarz*. Kraków 2007.

[4] *Biometria* [w:] Patrol - Magazyn Securitas w Polsce, nr 4, Warszawa 2007.

[5] Chałon M.: *Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych*. Wrocław 2007.

[6] Denning D.: *Wojna informacyjna i bezpieczeństwo informacji*. Warszawa 2002.

[7] Dutkiewicz W.: *Podstawy metodologii badań*. Kielce 2001.

[8] Dz. U. z 1997 r. Nr 133, poz. 883 ze zm.

[9] Dz. U. z 2006 r. Nr 143, poz. 1027 ze zm.

[10] Dz. Urz. z 29 grudnia 2004 r., UE L 385.

[11] Iskierka I., Iskierka S.: *Przegląd podstawowych technologii biometrycznych*. Częstochowa 2010.

[12] Kamiński A.: *Metoda, technika, procedura badawcza w pedagogice empirycznej*. [w:] Metodologia pedagogiki społecznej pod red. R. Wroczyńskiego i T. Pilcha, Wrocław 1974.

[13] Kaszubski R. W.: *Biometria w bankowości i administracji publicznej*. Warszawa 2010.

[14] Łobocki M.: *Metody badań pedagogicznych*. Warszawa 1978.

[15] Łobocki M.: *Metody i techniki badań pedagogicznych*. Warszawa 2000.

[16] Niedziejko P., Krysowaty I.: *Biometria. Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie* [w:] Zabezpieczenia nr 4, Warszawa 2006.

[17] Nowak S.: *Metodologia badań socjologicznych*. *Zagadnienia ogólne*. Warszawa 1970.

[18] Nowak S.: *Metodologia badań społecznych*. Lublin 1985.

[19] Tadeusiewicz R., Izworski A., Majewski J.: *Biometria*. Kraków 1993.

[20] Pieprzyk J., Hardjono T., Seberry J.: *Teoria bezpieczeństwa systemów komputerowych*. Gliwice 2005.

[21] Pieter J.: *Ogólna metodologia pracy naukowej*. Wrocław-Warszawa 1967.

[22] Pilch T.: *Organizacja procesu badawczego w pedagogicznych badaniach środowiskowych*. [w:] Metodologia środowiskowych badań pedagogicznych. Wrocław 1970.

[23] Pilch T: *Zasady badań pedagogicznych*. Warszawa 1995.

[24] Pilch T.: *Zasady badań pedagogicznych*. Wrocław- Warszawa - Kraków - Gdańsk 1977.

[25] Stasiak Ł., Czajka A., Strzelczyk P., Chochowski M., Pacut A.: *Od biometrii do bezpiecznej biometrii.* Warszawa 2007.

[26] Skorny Z.*: Prace magisterskie z psychologii i pedagogiki.* Lublin 1984.

[27] Wilson E.B.: *Wstęp do badań naukowych*. Warszawa 1964.

[28] Wiśniewski A.: *Metody oceny systemów rozpoznawania mówców*, Biuletyn IAiR WAT 2000, Nr 13.

[29] Zaczyński W.: *Praca badawcza nauczyciela*. Warszawa 1968.

[30] Zając P., Kwaśniowski S.: *Automatyczna identyfikacja w systemach logistycznych.* Wrocław 2004.

BIOMETRICS AS SECURITY FACTOR OF SEAFARERS

ABSTRACT

The article presents the basic issues related to the potential use and the use of biometric data. The studies lead to the conclusion that in the eyes of respondents biometric systems are quite well-known security systems that provide a high level of safety and facilitate everyday processes. On the other hand, these techniques are considered still too techniques suffer from high cost, leading to abuse of the data. Going further, it should be noted that the occurrence of respondents believe has the greatest range of financial services, and secure identity documents. The results show that the level of acceptance of biometric systems in the registration of time in organizations, they are also the ships, the user becomes a common thing today and undeniable, they become the same element of human resources management in any organization militarized.