Aleksandra BOBCOW, Mariusz DĄBKOWSKI
POLITECHNIKA GDAŃSKA, KATEDRA AUTOMATYKI

Biometryczna kontrola dostępu

Mgr inż. Aleksandra BOBCOW

Absolwentka Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej na kierunku Automatyka i Robotyka ze specjalnością Automatyka (2006). Słuchaczka Studium Doktoranckiego na tym wydziale od 2006 roku.

e-mail: a.bobcow@ely.pg.gda.pl

Dr inż. Mariusz DĄBKOWSKI

Jest adiunktem w Katedrze Automatyki na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej. Studia na tym samym wydziale ukończył w 2002 r. Stopień doktora nauk technicznych uzyskał w 2006 r. Przedmiotem jego zainteresowań naukowych jest robotyka, a w szczególności robotyka mobilna.

e-mail: m.dabkowski@ely.pg.gda.pl

Streszczenie

Opisano szczegółowo algorytm detekcji oraz identyfikacji człowieka na podstawie punktów nodalnych twarzy. Zdefiniowano pojęcia: biometria, proces pomiaru biometrycznego, metody biometrycznej identyfikacji oraz kontrola dostępu. Przedstawiono opis opracowanego systemu biometrycznej identyfikacji wykorzystującego sztuczne sieci neuronowe. Podano wyniki badań oraz przeprowadzono ich wnikliwą dyskusję.

Słowa kluczowe: Biometria, rozpoznawanie twarzy, kontrola dostępu.

Biometric access control

Abstract

Biometrics is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, a biometric authentication refers to technologies that measure and analyzes human physical and behavioral characteristics for authentication purposes. One of the most impressive examples of methods based on physical characteristics is facial recognition, which is the subject of this article. Biometric access control based on facial recognition system compare with other methods is not invasive, effective and easy in use that is why it was chosen. Human face is like a map with a lot of landmarks. Those special points make people exceptional. There are few main parts of the map which the program should identify: distance between eyes, width of nose, depth of eye sockets, cheekbones, mouth line and chin. After those measurements a person can be identified. The whole process of identification consists of five main steps: detection, alignment, normalization, representation and matching. The program was tested. Given results were satisfied. Non-braking development of IT section using biometrics will lead to the revolution of access control. In a few years people will not need a key, because they will already have one – the body.

Keywords: Biometrics, face recognition, access control.

1. Wstęp

W XXI wieku bezpieczeństwo staje się coraz bardziej zagrożone. Dynamiczny rozwój technologiczny doprowadził do wzrostu wartości dóbr materialnych. Ogromna konkurencja na rynku światowym spowodowała konieczność ochrony informacji, zaś narastająca fala terroryzmu i przestępczości przyczyniała się do wzmożonej ochrony społeczeństwa. Systemy zabezpieczeń, zarówno te globalne, jak i lokalne, stały się nieodzownym elementem życia ludzkiego. W 2006 roku powszechne stało się stosowanie systemów kontroli dostępu. Automatyczna identyfikacja wspiera zarządzanie przedsiębiorstwem, stanowi fundament do ochrony mienia oraz informacji. Przewiduje się, że nieustający postęp technologiczny pozwoli w najbliższych latach wyeliminować karty magnetyczne z zakodowanymi danymi osobowymi, ich nośnikiem zaś będą same osoby. Każdy człowiek jest jednostką niepowtarzalną. Ciało ludzkie może być zatem traktowane jako klucz dostępu. Jego biometryczna struktura jest nie do podrobienia. Powoduje to, iż automatyczna identyfikacja na podstawie metod biometrycznych stanowi pewny i bezpieczny sposób kontroli dostępu. W artykule przedstawiono system identyfikacji człowieka wykorzystujący metody biometryczne do rozpoznawania twarzy na podstawie cech geometrycznych.

2. Biometria

Biometria jest nauką zajmującą się zastosowaniem metod statystyki matematycznej w biologii, przede wszystkim do analizy danych liczbowych oraz do testowania modeli ma-tematycznych i hipotez teoretycznych dotyczących zmienności organizmów [1]. Obecnie biometria jest jedną z najlepiej rozwijających się technik informatyczno – elektronicznych. Metody biometryczne obejmują pomiary i selekcję indywidualnych, fizjologicznych lub behawioralnych cech organizmów żywych, a także udoskonalaniem metod pomiaru i wyboru najbardziej niepowtarzalnych osobniczo parametrów [2].

Proces pomiaru biometrycznego zapewnia dostarczenie fizycznych sygnałów wejściowych na strumień danych cyfrowych, które można poddać analizie programowej. Dane te stanowią podstawę decyzji dotyczącej podjęcia określonej akcji. W trakcie pomiaru można wyróżnić następujące etapy: rejestrację obrazu lub sygnału z obiektu biologicznego, przetwarzanie zarejestrowanego sygnału (filtracja), analizę programową – wyznaczanie parametrów charakterystycznych cech obiektu i zapamiętywanie ich (tworzenie zbioru parametrów, kodowanie, kompresja), rozpoznawanie – weryfikacja lub identyfikacja, czyli porównanie zbioru parametrów ze zbiorem parametrów wzorca a także podjęcie decyzji.

Każdy człowiek jest unikalną macierzą cech charakterystycznych, takich jak kontur twarzy, geometria dłoni czy wygląd tęczówki oka. Właśnie dzięki tym niezmiennym w czasie cechom można uzyskać biometryczne dane osobnika, które będą służyły do określania jego tożsamości. Istnieje wiele metod biometrycznych, ale do najbardziej znanych należą:

- rozpoznawanie linii papilarnych,
- tęczówki bądź też siatkówki oka,
- geometrii dłoni,
- cech charakterystycznych twarzy,
- mowy,
- charakteru pisma.

Ze względu na łatwość w użyciu oraz efektywność metoda biometrycznej identyfikacji na podstawie charakterystycznych cech geometrii twarzy jest tematem niniejszego artykułu.

Kontrola dostępu obejmuje mechanizmy nakładania restrykcji na dostęp do systemu lub jego części w celu ochrony znajdujących się na nim zasobów. Procedury kontroli dostępu służą do nadawania lub odbierania prawa dostępu danego użytkownika do zasobu. Ochrona zasobu jest realizowana poprzez ograniczenia dostępu tylko w odniesieniu do użytkowników uwierzytelnionych i autoryzowanych [3]. System kontroli dostępu składa się z: centrali – kontrolera, która stanowi serce systemu i jest elementem decyzyjnym procesu, czytników kart magnetycznych, zbliżeniowych,

Wieganda czy biometrycznych urządzeń zabezpieczających, takich jak: zwory i rygle elektromagnetyczne, przyciski wyjścia, przyciski do awaryjnego otwierania drzwi, solenoidy, samozamykacze drzwi, oprogramowania opisanego w dalszej części artykułu.

Proces biometrycznej identyfikacji jest niezwykle skomplikowany, dlatego niezbędne jest użycie odpowiedniego narzędzia. Równoległe przetwarzanie wielu informacji jednocześnie oraz zdolność uogólniania wiedzy dla nowych, nieznanych wcześniej wzorców pozwoliła wykorzystać sztuczne sieci neuronowe jako narzędzie do biometrycznej identyfikacji. Zastosowanie sieci o strukturze wielowarstwowej, składającej się z trzech warstw: wejściowej, ukrytej i wyjściowej, umożliwiło zaprojektowanie systemu rozpoznawania osób na podstawie ich charakterystycznych cech twarzy.

3. Biometryczny system detekcji i identyfikacji twarzy [4]

Do opracowania systemu do biometrycznej kontroli dostępu wykorzystano zintegrowane środowisko programistyczne Delphi. Charakteryzuje się ono możliwością szybkiego tworzenia aplikacji (ang. *RAD – Rapid Application Development*). Program składa się z dwóch części: algorytmu detekcji twarzy oraz algorytmu identyfikacji twarzy. Algorytm detekcji twarzy zawiera 11 etapów:

- konwertowanie obrazu do odcieni szarości,
- wygładzanie,
- wykrywanie krawędzi,
- wypełnianie konturu,
- eliminacja tła,
- detekcja obszaru twarzy,
- detekcja oczu,
- detekcja źrenic,
- detekcja nosa,
- detekcja ust,
- obliczanie wartości biometrycznych twarzy.

Na wstępie fotografia jest konwertowana do odcieni szarości. Natężenie bieli zawiera się w przedziale od 0 do 255 (0 – czarny, 255 biały). Obliczania wykonuje się dla każdego piksela osobno i wyraża się jako średnią arytmetyczną składowych R, G i B (każda składowa zawiera się w przedziale od 0 do 255). Ponieważ do dalszego filtrowania obrazu jest potrzebna wartość całkowita, wartości dziesiętne są pomijane.

Następnie fotografia poddawana jest dwuwymiarowemu filtrowi powodującemu wygładzenie obrazu (efekt rozmycia). Zastosowanie tego filtru umożliwia usunięcie chropowatości i szumów przeszkadzających przy dalszej analizie obrazu. Kolejne dwa filtry dwuwymiarowe umożliwiają wykrycia krawędzi.

Przetworzony obraz składa się z m linii po n pikseli każda. Każda i-ta linia jest skanowana począwszy od pierwszego piksela dopóki wartość badanego piksela jest równa 0. Dla pierwszej niezerowej wartości piksela odczytywane są współrzędne $[k_P,i]$. Następnie i-ta linia skanowana jest od piksela n-tego wstecz dopóki wartość badanego piksela jest równa 0. Dla pierwszej niezerowej wartości odczytywane są współrzędne $[k_K,i]$. Dla każdej skanowanej linii rysowany jest biały odcinek o współrzędnych $A[k_P,i]$ i $B[k_K,i]$. W ten sposób wykryty kontur zostaje wypełniony białymi odcinkami. Powstały kształt nazywa się maską konturu. Porównanie oryginalnej fotografii do maski konturu dla każdego białego piksela maski, skutkuje pozostawieniem oryginalnej wartości piksela fotografii, natomiast każdy inny piksel fotografii zamieniany jest na czarny. Zabieg ten umożliwia wstępne odseparowanie obrazu twarzy od tła.

Zidentyfikowanie odcienia barwy każdego piksela fotografii pozwala określić obszar twarzy. Zadanie to jest trudne do osiągnięcia podczas stosowania standardowego opisu RGB koloru piksela. Nie istnieje jedna składowa określająca barwę, lecz jest ona wynikiem zmieszania wszystkich trzech składowych. Istnieje sposób opisu koloru piksela HSV umożliwiający identyfikację barwy, ponieważ tylko składowa H odpowiada za barwę piksela, natomiast składowe S i V za odcień barwy. Przeprowadzone badania pozwoliły ustalić, że składowe S<16 i V<37 dla dowolnego H opisują barwy o małym nasyceniu zbliżone do odcieni szarości. Kolory takie nie występują w obszarach twarzy. Zaobserwowano również, że piksele należące do białek, tęczówek i źrenic zawsze posiadają składowe S<16 i V<37. Każdy piksel fotografii przekonwertowano z opisu RGB do HSV i zaznaczono na czerwono tylko te piksele, których składowa S>16 i V>37. Pozwoliło to na określenie obszaru twarzy z wyseparowaniem oczu. Po eliminacji zbędnych szumów otrzymuje się obszar oczu stanowiący element wyjściowy do dalszych etapów detekcji twarzy.

Zaobserwowano, że na zdjęciu wykonanym przy użyciu lampy błyskowej w źrenicach zawsze tworzy się biały refleks. Na podstawie badań dostępnych zdjęć twarzy zdefiniowano przedziały natężenia bieli określające źrenice i otaczające je tęczówki. Refleks w źrenicy określono doświadczalnie jako piksele o natężeniu bieli większym, niż 72%, czyli wartości większej niż 184 w przedziale od 0 do 255. Otoczenie źrenicy określono jako piksele o natężeniu bieli mniejszym, niż 39%, czyli wartości mniejszej niż 101 w przedziale od 0 do 255. Ostatecznie pomiędzy wykrytymi źrenicami poprowadzono linię.

Następnie obliczono równanie prostej

$$l: y=ax+b \tag{1}$$

prostopadłej i przechodzącej przez środek odcinka $\overline{AB}$ wyznaczonego przez punkty $A=[x_L,y_L]$ (środek oka lewego) oraz $B=[x_R,y_R]$ (środek oka prawego). Przekonwertowano oryginalną fotografię na odcienie szarości, a następnie wygładzono stosując filtry dwuwymiarowe. Badania pozwoliły stwierdzić, że pierwsze minimum znajdujące się za najwyższą wartością funkcji zawsze odpowiada cieniowi rzucanemu przez nos. Ten punkt jest uznany jako charakterystyczny przy ustaleniu położenia nosa. Po przeprowadzeniu wielu doświadczeń ustalono, że środek ust jest pierwszym minimum po minimum ustalonym jako położenie nosa.

Analiza fotografii pozwoliła otrzymać następujące punkty charakterystyczne:

- współrzędne środka pierwszej
- współrzędne środka drugiej źrenicy,
- współrzędne nosa
- współrzędne ust
- współrzędne punktu S, który jest punktem przecięcia prostej łączącej źrenice z prostą prostopadłą, na której leżą współrzędne nosa i ust.

Na podstawie uzyskanych punktów charakterystycznych obliczono wartości, których stosunki są danymi biometrycznymi twarzy przedstawianymi sieci neuronowej w celu identyfikacji. Efektem końcowym analizy fotografii jest otrzymanie następujących punktów charakterystycznych zestawionych w tablicy 1.

Tab. 1. Punkty charakterystyczne
Tab. 1. Characteristics points

Oznaczenie	Opis punktów charakterystycznych
$A = [x_L,y_L]$	współrzędne środka pierwszej źrenicy
$B = [x_R,y_R]$	współrzędne środka drugiej źrenicy
$P_N = [x_{NOS},y_{NOS}]$	współrzędne nosa
$P_U = [x_{USTA},y_{USTA}]$	współrzędne ust
$S = [x_{SR},y_{SR}]$	od punktu przecięcia prostej l ze środkiem odcinka $\overline{P_N P_U}$

Na podstawie uzyskanych punktów charakterystycznych obliczono zestawione w tablicy 2 wartości.

Tab. 2. Wartości obliczone dzięki punktom charakterystycznym
Tab. 2. Values calculated from characteristics points

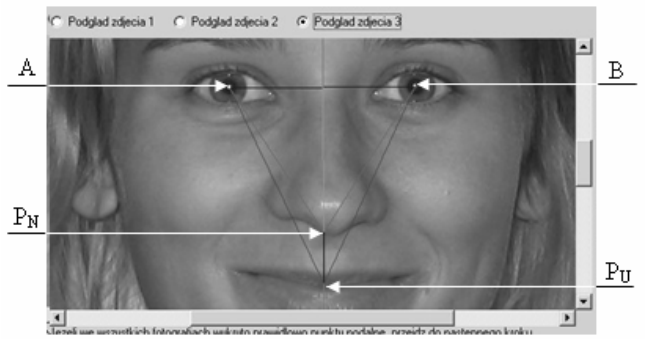
Oznaczenie	Opis
$O = \|AB\|$	Odległość oczu
$N = \|SP_N\|$	Odległość nosa od punktu przecięcia prostej l ze środkiem odcinka $\overline{AB}$
$U = \|SP_U\|$	Odległość ust od punktu przecięcia prostej l ze środkiem odcinka $\overline{AB}$
$J=U–N$	Odległość nosa od ust
KN	kąt zawarty między odcinkami $\overline{\boldsymbol{P}_N\boldsymbol{A}}$ i $\overline{AB}$
KU	kąt zawarty między odcinkami $\overline{\boldsymbol{P}_U\boldsymbol{A}}$ i $\overline{AB}$

Znając wartości elementów zestawionych, w tablicy 2 obliczono następujące stosunki,

$$C = \frac{N}{O}, D = \frac{U}{O}, T = \frac{N}{U}, R = \frac{O}{U}, E = \frac{KN}{90}, I = \frac{KU}{90} \qquad (2)$$

które są danymi biometrycznymi twarzy przedstawianymi sieci neuronowej w celu identyfikacji.

Graficzne przedstawienie pracy algorytmu zostało pokazane na rys. 1.



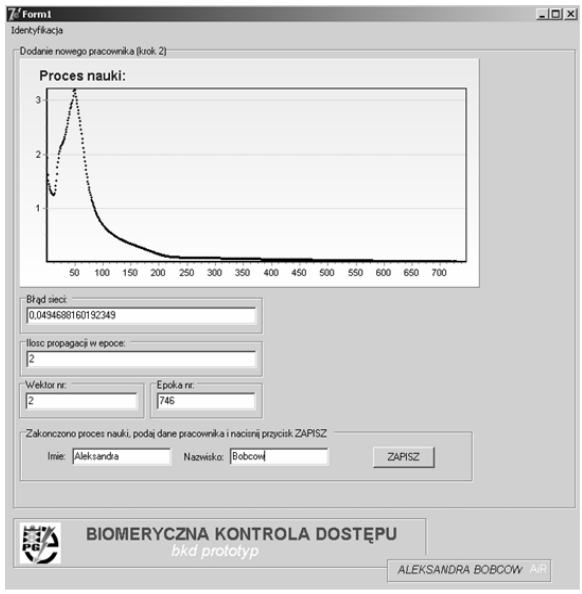
Rys. 1. Efekt końcowy zastosowania algorytmu detekcji i rozpoznawania twarzy
Fig. 1. Final face detection and recognition effect

Proces identyfikacji jest dokonywany z wykorzystaniem zaprojektowanej trójwarstwowej sztucznej sieci neuronowej działającej na zasadzie perceptronu wielowarstwowego ze sprzężeniem zwrotnym. W warstwie wejściowej znajduje się sześć neuronów, w warstwie ukrytej cztery, a w warstwie wyjściowej trzy. Uczenie sieci polega na przedstawieniu sieci neuronowej danych biometrycznych trzech fotografii tej samej osoby. Początkowe wartości wag połączeń sieci neuronowej zostały wybrane w sposób losowy. Ustalanie odpowiednich wartości wag podczas uczenia odbywa się iteracyjnie metodą wstecznej propagacji błędów. Na podstawie badań przyjęto, że sieć została wytrenowana, jeżeli w dwóch iteracjach błąd sieci dla danej epoki będzie niższy od założonej wartości 0,05.

Projekt systemu do identyfikacji człowieka na podstawie jego cech charakterystycznych twarzy został wykonany przy wykorzystaniu fotografii wykonanych za pomocą dwóch aparatów cyfrowych: Canon PowerShot A70 i Sony DSC-V1.

4. Badania weryfikacyjne systemu [4]

Aplikacja komputerowa zawiera dwie podstawowe funkcje: dodawanie nowego pracownika oraz identyfikację pracownika. Po uruchomieniu opcji dodania nowego pracownika pojawia się okno dialogowe, należy wybrać trzy twarze zapisane w formacie „bmp". Kolejnym krokiem jest rozpoznanie danych biometrycznych. W trakcie nauki sieci jest rysowany wykres przedstawiający ilość propagacji potrzebnych do uzyskania błędu epoki mniejszego niż założony. Na bieżąco są podawane również takie wartości jak błąd sieci dla aktualnie badanej epoki, liczbę propagacji w epoce, numer aktualnie badanego wektora wejściowego oraz numer aktualnej epoki. Jeżeli wszystkie trzy twarze zostały poprawnie rozpoznane, ostatnim etapem jest zapisanie danych biometrycznych pracownika oraz dodanie go do bazy danych. Okno dialogowe programu jest przedstawione na rys. 2.



Rys. 2. Okno dialogowe dodawania nowego pracownika
Fig. 2. Adding new worker dialogue window

Identyfikacja pracownika polega na załadowaniu jednego obrazu twarzy i rozpoznaniu cech biometrycznych. Jeżeli twarz została poprawnie rozpoznana pojawi się werdykt sieci: czy pracownik został rozpoznany. Jeśli tak, pojawią się również jego dane (imię i nazwisko), w przeciwnym przypadku pojawi się komunikat „twarz nierozpoznana".

Badania weryfikacyjne aplikacji przeprowadzone na grupie 20 osób, pozwoliły stwierdzić, że program jest obarczony 10% błędem. W dwóch przypadkach została dokonana błędna identyfikacja – twarz została nierozpoznana, mimo że znajdowała się w bazie danych. Czas identyfikacji zawiera się w granicach od 0,5 do 1 minuty. Proces dodawania nowego pracownika trwa w granicach 0,7 do 2 minut w zależności od zestawu twarzy poddanych detekcji.

Testy wykazały, że niektóre twarze nie były poprawnie wykrywane w procesie detekcji cech biometrycznych. Jest to związane z błędnym określeniem punktów nodalnych w przypadku, kiedy osoba poddająca się identyfikacji nosi okulary (refleksy w nieodpowiednich punktach), jak również posiada silny zarost.

Ponadto nieznane są potencjalne wyniki badań dla przedstawicieli innej rasy niż kaukaska, np. podczas analizy twarzy osób o ciemnym kolorze skóry.

Duży wpływ na jakość rozpoznawania ma liczba wykrywanych punktów nodalnych. Jej zwiększenie spowodowałoby zmniejszenie błędu identyfikacji.

5. Podsumowanie

Wprowadzenie biometrycznych systemów identyfikacji zrewolucjonizowało zarządzanie na skalę globalną. W 2005 roku powstawały pierwsze programy umożliwiające identyfikację na podstawie cech charakterystycznych twarzy. Natomiast już rok później zaczęto wprowadzać biometryczne paszporty oraz systemy biometrycznej identyfikacji do fabryk, przedsiębiorstw, małych i dużych firm. Poczucie bezpieczeństwa w dobie niepewności stało się bezcenne. Natomiast biometryczna kontrola dostępu jest

jedną z najpewniejszych dróg do jego osiągnięcia. Według autorów czasopisma „global identification" biometryczna identyfikacja jest uznawana za jedyną pewną i bezpieczną drogę rozpoznawania istot żywych, zarówno zwierząt jak i ludzi [5].

Istniejące systemy biometrycznej kontroli dostępu opatrzone są tajemnicą. W chwili obecnej w literaturze nie są zawarte szczegółowe informacje dotyczące rozwiązań biometrycznej identyfikacji, stąd też powstała konieczność zaprojektowania w tym celu aplikacji komputerowej. W artykule przedstawiono jedną z wielu możliwych dróg umożliwiających identyfikację na podstawie charakterystycznych cech twarzy. Problem ten jest niezwykle złożony. Opisany program nie jest w 100% niezawodny, jednak otrzymane wyniki są obiecujące. Aplikacja ta stanowi punkt wyjścia do opracowania w pełni funkcjonalnego i bardziej niezawodnego systemu biometrycznej kontroli dostępu. Pierwszym etapem do osiągnięcia tego celu byłoby zwiększenie liczby wykrywanych punktów nodalnych.

6. Literatura

[1] Nowa Encyklopedia Powszechna PWN, tom 1, Wydawnictwo Naukowe PWN, Warszawa 1995.
[2] Sławiński Jerzy, Gomulska Elżbieta, Plucińska Mirosława, Rozbici Leon, Wójtowicz Jarosław, „Metody biometryczne dla zwiększenia bezpieczeństwa kontroli dostępu do pomieszczeń i zasobów komputerowych oraz uwierzytelniania osób", Wydawnictwo Warszawa 2002.
[3] Portal Kontrola Dostępu, http://www.kontrola-dostepu.pl/ z 22 marca 2006 roku.
[4] Bobcow Aleksandra, praca magisterska „Biometryczna kontrola dostępu", Politechnika Gdańska, Wydział Elektrotechniki i Automatyki, 2006 rok
[5] Global identification, on publishing, July 2006

Artykuł recenzowany

INFORMACJE

Studia Podyplomowe

Wydział Elektryczny Politechniki Śląskiej w Gliwicach
Instytut Metrologii, Elektroniki i Automatyki
ogłasza nabór na Dwusemestralne Zaoczne Studia Podyplomowe

Organizacja i Akredytacja Laboratoriów

Cel studiów

Celem studiów jest pogłębienie wiedzy w zakresie systemu jakości laboratoriów wzorcujących, problematyki zapewnienia jakości wyposażenia pomiarowego, walidacji metod pomiarowych, metodyki tworzenia budżetów niepewności i opracowania wyników badań zgodnie z obowiązującymi przepisami oraz przygotowanie słuchaczy do samodzielnej pracy w zakresie organizowania i prowadzenia laboratorium akredytowanego. Przedstawione zostaną podstawy automatyzacji pomiarów i organizacji systemów pomiarowych. Problemy analizowane będą na przykładach, z uwzględnieniem niezbędnych podstaw teoretycznych oraz aktualnych przepisów.

Profil uczestnika studiów

Studia przeznaczone są dla pracowników o różnych specjalnościach, zajmujących się organizacją laboratoriów oraz wykonywaniem badań i kalibracji w zakładach, firmach lub jednostkach naukowo-badawczych. Studia adresowane są do osób z wyższym wykształceniem zajmujących się realizacją pomiarów i opracowywaniem wyników badań w różnych dziedzinach. Ich ukończenie pozwoli uczestnikom na podwyższenie kwalifikacji niezbędnych do efektywnego opracowywania i dokumentowania procesów pomiarowych. Absolwent studiów otrzymuje Świadectwo Ukończenia Studiów Podyplomowych w zakresie objętym nazwą studiów.

Studia prowadzone są na Wydziale Elektrycznym Politechniki Śląskiej w Gliwicach, w systemie zaocznym w każdą sobotę lub w co drugi weekend (do wyboru) przez dwa semestry. Zajęcia prowadzone są przez nauczycieli akademickich ze stopniem co najmniej doktora oraz przez zaproszonych Gości o uznanym dorobku i autorytecie. Studia obejmują 200 godzin dydaktycznych. Rozpoczęcie Studiów nastąpi po skompletowaniu odpowiedniej liczby kandydatów na dany rodzaj studiów.

Warunki przyjęcia na studia:

1. Na studia mogą być przyjęte osoby posiadające dyplom magistra lub inżyniera, posiadające podstawową wiedzę z zakresu wybranych studiów.
2. Warunkiem uruchomienia studiów jest przyjęcie odpowiedniej liczby Kandydatów na podstawie złożonych dokumentów.
3. Dokumenty składane przez Kandydatów:
   - Kwestionariusz Osobowy – Karta Zgłoszenia (do pobrania ze strony internetowej). Przyjmowane na bieżąco: e-mailem, pocztą lub osobiście.
   - Kopia/odpis dyplomu ukończenia studiów wyższych.
4. Kandydaci odbywają rozmowę kwalifikacyjną. Termin ustalony i podany zostanie po skompletowaniu odpowiedniej liczby Kandydatów.
5. Po spełnieniu warunków Kandydaci wnoszą opłatę zgodnie z zawartą umową w wysokości 3 800 złotych za cały okres studiów.

Organizator studiów:

Instytut Metrologii, Elektroniki i Automatyki Politechniki Śląskiej, 44-100 Gliwice, ul. Akademicka 10, tel. 032 237 12 41, fax: 032 237 20 34, e-mail: re2@polsl.pl lub anna.kropka@polsl.pl, http://www.wega.elektr.polsl.gliwice.pl

Kierownik studiów:

Prof. dr hab. inż. Tadeusz SKUBIS