Jacek Paś

Diagnozowanie systemu multibiometrycznego dla wybranego obiektu transportowego

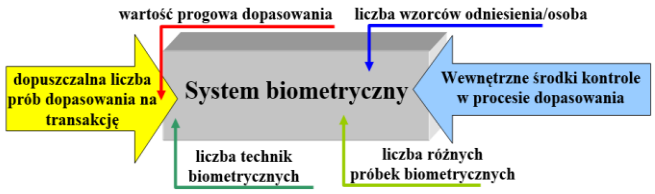
JEL: L91 DOI: 10.24136/atest.2018.457
Data zgłoszenia: 19.11.2018 Data akceptacji: 15.12.2018

Systemy multibiometryczne stosowane w obiektach transportowych w przeciwieństwie do „zwykłych" systemów biometrycznych wykorzystują kilka technik rozpoznania, np. odcisku palca, tęczówki, głosu lub twarzy. Urządzenia biometryczne niekiedy stanowią część składową elektronicznych systemów bezpieczeństwa. Systemy te są obecnie instalowane w wielu obiektach transportowych – stacjonarnych i niestacjonarnych gdzie występuje duże natężenie ruchu osobowego. Urządzenia te stosuje się dla terenów najczęściej rozległych obszarowo, port lotniczy, baza logistyczna lub dworzec kolejowy. W artykule przedstawiono zagadnienia dotyczące stanowiska diagnostycznego dla systemu biometrycznego który w swojej strukturze posiada klika prostych technik identyfikacyjnych.

Słowa kluczowe: biometria, eksploatacja, diagnostyka, techniki rozpoznania, odcisk palca.

Wstęp

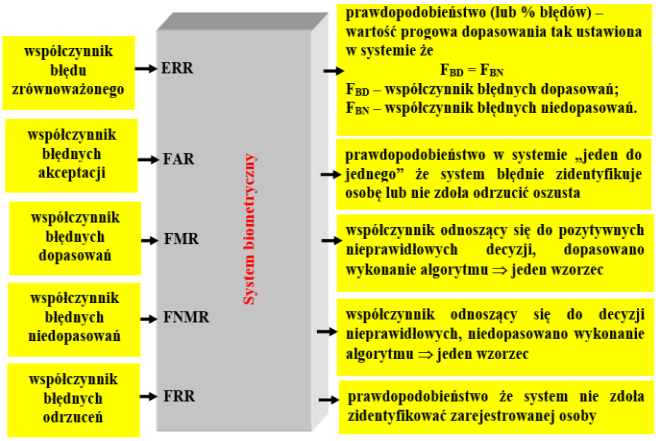
Biometria to czynnik tożsamości - „coś czym jesteś lub coś co możesz zrobić" stosowana na potrzeby fizycznego i logicznego dostępu [1,2,8]. Dostęp logiczny – obejmuje dostęp do aplikacji, usług lub pełnomocnictw – rys. 1.



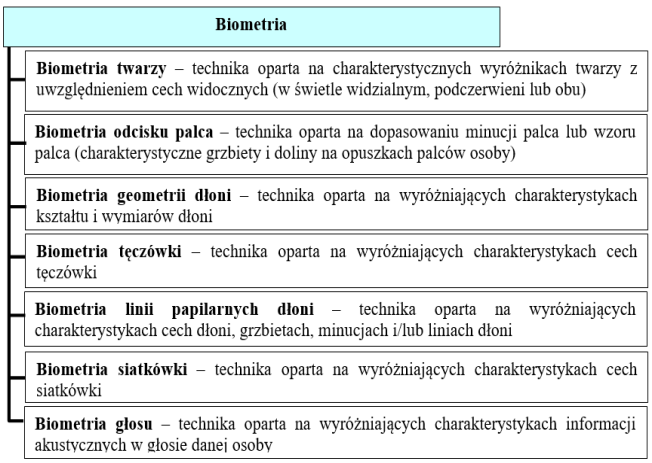
Rys. 1. System biometryczny [źródło: opracowanie własne]

Według normy ISO/IEC 27001 (PN-ISO/IEC 27001:2007) w systemach biometrycznych można wyróżnić następujące procesy:

- adaptowanie – proces zautomatyzowanego aktualizowania lub odświeżania wzorca informacji;
- próba – przedłożenie próbki biometrycznej pobranej od osoby w celu zarejestrowania, zweryfikowania tożsamości lub zidentyfikowania w systemie biometrycznym;
- grupowanie – dzielenie bazy danych na podstawie informacji zawartych we wzorcach biometrycznych;
- cecha biometryczna – mierzalna biologiczna lub behawioralna charakterystyka, która w wiarygodny sposób odróżnia jedną osobę od drugiej, stosowana w celu ustalenia albo zweryfikowania zadeklarowanej tożsamości zarejestrowanej osoby;
- uwierzytelnienie biometryczne – proces potwierdzenia tożsamości osoby metodą weryfikowania lub identyfikowania;
- dane biometryczne – informacje wyodrębnione z próbki biometrycznej i stosowane do utworzenia wzorca odniesienia lub dopasowania;
- identyfikowanie biometryczne – proces porównywania „jedna do wielu" przedłożonej próbki biometrycznej z niektórymi lub wszystkimi zarejestrowanymi wzorcami odniesienia w celu ustalenia tożsamości osoby – rys. 2;
- polityka stosowania biometrii – zbiór zasad określający zastosowanie wzorca biometrycznego w konkretnej społeczności, klasie zastosowań o wspólnych wymaganiach bezpieczeństwa – rys. 3;
- regulamin stosowania biometrii – zestawienie procedur stosowanych przez organizację podczas cyklu życia wzorca biometrycznego;
- próbka biometryczna – początkowe (surowe) dane biometryczne (pobierane i przetwarzane);
- system biometryczny – zautomatyzowany system który może pobierać, wyodrębniać, dopasowywać i zwracać decyzję /dopasowano - niedopasowano/;
- weryfikowanie biometryczne – proces sprawdzania zgodności wzorca dopasowanego z określonym wzorcem odniesienia wybranym na podstawie zadeklarowanej tożsamości;
- polityka decyzyjna – logika stosowana przez system w celu podejmowania decyzji – dopasowano/niedopasowano.



Rys. 2. Definicja podstawowych współczynników i parametrów systemu biometrycznego [źródło: opracowanie własne]

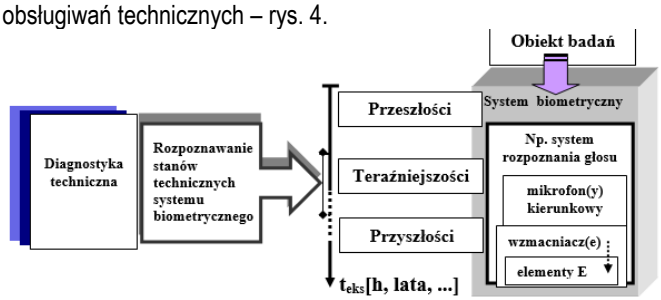


Rys. 3. Podział systemów biometrycznych według norm [źródło: opracowanie własne]

1. Podstawowe pojęcia dotyczące diagnozowania systemów biometrycznych

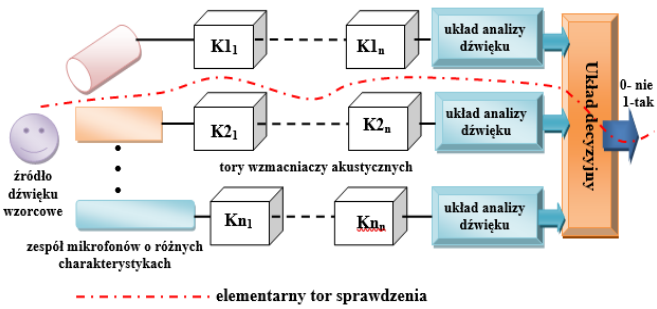
W zintegrowanym systemie biometrycznym czynnikiem stymulującym bezpośrednio rozwój diagnostyki jest odpowiedzialność za funkcję realizowaną przez system.

Diagnostykę techniczną można zdefiniować jako *„zorganizowany zbiór metod i środków do oceny stanu technicznego”* w zintegrowanych systemów biometrycznych [1,3,7]. W większości są to systemy działaniowe, celowo zaprojektowane dla wykonania określonej misji np. dane biometryczne uważane za wzorzec odniesienia umieszczone w pamięci komputera, generujące lub transformujące informacje, które są wykorzystywane do oceny ich stanu technicznego. Potrzeba stosowania diagnostyki znajduje swoje uzasadnienie w modelu destrukcji systemu biometrycznego – wiąże się to z czasem istnienia obiektu, poziomem konstrukcji, nowoczesności technologii wytwarzania, intensywności użytkowania oraz jakości obsługiwań technicznych – rys. 4.



Rys. 4. Zależności występujące w diagnostyce technicznej systemów biometrycznych [źródło: opracowanie własne]

Ważnym pojęciem związanym z planowaniem badań diagnostycznych jest pojęcie sprawdzenia d_j. Przez sprawdzenie d_j (j=1, r) rozumiemy ciąg czynności służących zbadaniu określonej cechy obiektu – w tym przypadku systemu biometrycznego. Aby zrealizować sprawdzenie systemu biometrycznego należy odpowiednio przygotować system do badania. Oznacza to że należy podać na jego wejście(a) sygnały pobudzające tj. wzorcowe dane biometryczne – np. DNA, wzorzec twarzy lub wzorzec próbki głosu i dokonać pomiaru sygnału(ów) odpowiedzi oraz porównać ich odpowiedzi z dopuszczalnymi. W zależności od liczby badanych podsystemów biometrycznych (niezależnych torów biometrycznych wykorzystujących do identyfikacji człowieka różne zjawiska fizyczne) w torze sprawdzenia możemy wyróżnić sprawdzenia elementarne lub kompleksowe [2,4,11]. Torem sprawdzenia kompleksowego d_j nazywamy podzbiór $E_j \subset E$ tych elementów systemu biometrycznego, które mają wpływ na wartość badanej odpowiedzi, a zatem i na wynik sprawdzenia kompleksowego d_j – rys. 5.



Rys. 5. Tor sprawdzenia w biometrycznym systemie rozpoznawania głosu [źródło: opracowanie własne]

W przypadku gdy różne tory sprawdzeń zawierać będą elementy wspólne, wówczas tory takie nazywamy przecinającymi się, w przeciwnym przypadku (brak elementów wspólnych) nazwiemy je nieprzecinającymi się lub rozłącznymi.

Wynik porównania sygnału odpowiedzi z odpowiedziami dopuszczalnymi czyli wynik sprawdzenia d_j w realnych badaniach jest funkcją:

- aktualnej wartości kontrolowanej cechy systemu biometrycznego, a więc i stanu elementów objętych sprawdzeniem – sprawdzenie elementarne rys. 5; lub sprawdzenie kompleksowe obejmujące cały system biometryczny rozpoznawania głosu – tzn. wszystkie kanały przetwarzania dźwięku;
- dokładności użytych przyrządów kontrolno-pomiarowych w tym użytych w systemie przetworników fali akustycznej na sygnał dźwiękowy tzn. mikrofonów;
- występujących zakłóceń podczas realizacji sprawdzenia – np. poziom hałasu (tła) występującego wokół biometrycznego systemu rozpoznania głosu;
- stopnia wyszkolenia, doświadczenia i odporności na zakłócenia osób wykonujących pomiary, badania w przypadku systemu ręcznego lub półautomatycznego [7,10,16].

Podczas wykonywania sprawdzeń systemu biometrycznego mogą wystąpić dwa rodzaje błędów:

- **błąd I rodzaju,** polegający na uznaniu odpowiedzi dopuszczalnej za niedopuszczalną;
- **błąd II rodzaju,** polegający na uznaniu odpowiedzi niedopuszczalnej za dopuszczalną.

Jeżeli przyjmiemy pełną wiarygodność wykonywanych sprawdzeń to będzie oznaczało brak występowania błędów zarówno I jak i II rodzaju. Wynik sprawdzenia pozytywny $D_j = D_j^1$, gdy wartość kontrolowanej cechy (np. głos, obraz) zawierać się będzie tylko w przedziale wartości dopuszczalnych. W przeciwnym wypadku wynik sprawdzenia będzie negatywny ($D_j = D_j^0$).

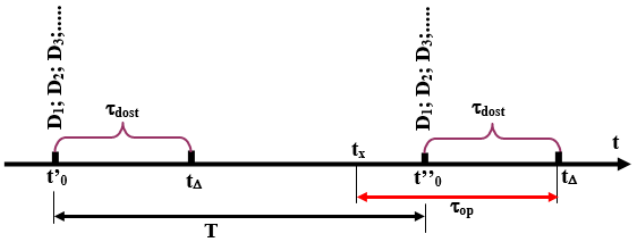
Pozytywny wynik sprawdzenia oznacza także brak występowania w torze sprawdzenia elementów niezdatnych, natomiast wynik negatywny oznacza że wśród elementów toru sprawdzenia systemu ochrony istnieje przynajmniej jeden element niezdatny.

Wykonanie określonego sprawdzenia d_j systemu wymaga:

- określonego czasu $\tau_j = \tau(d_j)$, na które składają się czasy wykonania wszystkich elementarnych czynności niezbędnych od zrealizowania sprawdzenia toru(ów) biometrycznego systemu rozpoznania głosu – rys. 5;
- poniesienia określonych kosztów $c_j = c_j(d_j)$, związanych np. z amortyzacją przyrządów kontrolno-pomiarowych, użyciem dodatkowej energii, koszty osobowe, itp.

W zależności od celu badań wyróżnia się cztery rodzaje badania stanu systemów biometrycznych [2,3,11]:

1. **diagnozowanie** – badanie polegające na podjęciu decyzji odnośnie dalszego postępowania z systemem biometrycznym bezpośrednio po zakończeniu badania [7,9,11]. Jeżeli celem jest rozpoznanie zdatności bądź niezdatności systemu biometrycznego wówczas takie badanie można nazwać **kontrolą zdatności**. W przypadku systemów biometrycznych kontrola zdatności jest wykonywana podczas przygotowania systemu do użytkowania. Wykonuje się ją także w czasie wykonywania i po zakończeniu prac okresowych (przeglądach); po naprawach, w czasie magazynowania systemu – okresowo [5,6,7,14]. Jeżeli celem badania jest określenie który element systemu jest niezdatny, wówczas takie badanie diagnostyczne nazywamy **lokalizacją uszkodzeń**.
2. **dozorowanie** – ciągła kontrola systemu biometrycznego i dostarczanie użytkownikowi z małym opóźnieniem informacji o każdej zmianie stanu systemu biometrycznego. Dozorowanie może odbywać się **równolegle** (jednocześnie opracowywane wyniki sprawdzeń) – rys. 6, lub **sekwencyjnie** (niejednocześnie – wypadkowa diagnoza po realizacji wszystkich sprawdzeń) – rys. 7.



Rys. 6. Dozorowanie równolegle systemu biometrycznego [źródło: opracowanie własne]

Dozorowanie równoległe jest to działanie, dla którego jest słuszna implikacja (1)

$$[R(\{D_k\}, \{e_n\}) \wedge D_1(t_0 + \tau_{dost})] \Rightarrow \Delta\tau_{op}\, e_1(t_0) \quad (1)$$

oraz $\tau_{dost} < \tau_{op} < \tau_{dost} + T$,

gdzie:

τ_{dost} – zwłoka dostarczenia diagnozy użytkownikowi (suma czasu potrzebnego na wygenerowanie diagnozy oraz czasu na przesłanie jej użytkownikowi);

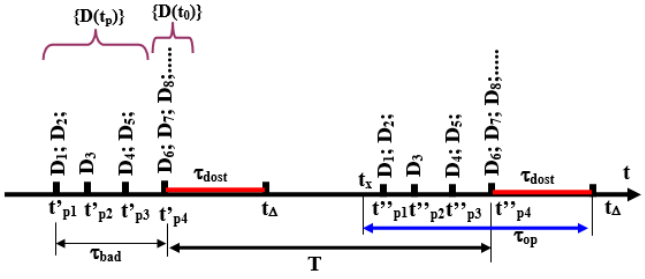
τ_{op} – zwłoka dostarczenia informacji o zmianie stanu (czas między chwilą zmiany stanu a chwilą dostarczenia informacji o tym użytkownikowi);

T – okres dozorowania (powtarzania się operacji dozorujących);

$D_1(t_0 + \tau_{dost})$ – zestaw objawów uzyskanych w chwili t_0, lecz wykorzystany ze zwłoką τ_{dost};

$\Delta\tau_{op}\, e_1(t_0)$ – diagnoza chwilowa stanu w chwili t_x poprzedzającej t_0 i dostarczona użytkownikowi ze zwłoką τ_{op}

W tym przypadku diagnoza chwilowa wynika ze zbioru D_1 objawów uzyskanych tylko w chwili t_0.



Rys. 7. Dozorowanie sekwencyjne systemu biometrycznego [źródło: opracowanie własne]

Istnieje tu możliwość, że w chwili t_0 wyniki $D(t_p)$ są już częściowo nieaktualne (wartości odpowiednich parametrów uległy zmianie). Zmniejsza to wiarygodność diagnozy chwilowej.

Dla dozorowania sekwencyjnego słuszna jest implikacja (2)

$$[R(\{D_k\}, \{e_n\}) \wedge D_1(t_p + \tau_{dost}) \wedge D_1(t_0 + \tau_{dost})] \Rightarrow \Delta\tau_{op}\, e_1(t_0) \quad (2)$$

oraz $\tau_{dost} < \tau_{op} < \tau_{dost} + T + \tau_{bad}$;

gdzie:

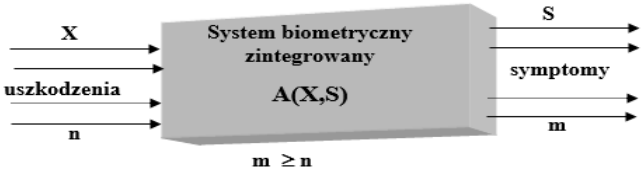
$D_1(t_p + \tau_{dost})$ – zbiór wyników sprawdzeń uzyskanych w chwilach t_p poprzedzających t_0; lecz wykorzystany ze zwłoką τ_{dost};

τ_{bad} – czas realizacji cyklu sprawdzeń.

3. **genezowanie** – rozpoznawanie przyczyn aktualnego stanu systemu biometrycznego, na podstawie wiarygodnej diagnozy o aktualnym stanie systemu biometrycznego. Szczególne znaczenie w przypadku uszkodzeń mających charakter katastroficzny.
4. **prognozowanie** – przewidywanie zdarzeń przyszłych na podstawie zdarzeń dotychczasowych. Z prognozowaniem związane są dwa pojęcia:
   - **zakres badań systemu** biometrycznego – jego miara to stosunek liczby istotnych cech systemu sprawdzanych podczas badań do ogólnej liczby tych cech określających zdatność obiektu (lub inaczej stosunek liczby elementów systemu objętych sprawdzeniami do ogólnej liczby wyróżnionych elementów systemu);
   - **głębokość badań systemu biometrycznego** – określa stopień podziału systemu na elementy, z dokładnością do stanu których uzyskuje się informację w wyniku badania – rys. 6, 7.

2. Diagnozowanie zintegrowanych systemów biometrycznych – przykłady rozwiązań

Ogólną istotę diagnozowania systemu biometrycznego (rys. 8) można przedstawić jako poszukiwanie związków pomiędzy stanem X_n a generowanymi sygnałami diagnostycznymi S_m systemu biometrycznego z pominięciem oddziaływań zewnętrznych [10,12,15]. Dla tak rozpatrywanej diagnostyki systemu można zbudować tablicę obserwacji (rys. 9), gdzie umieszczamy zestaw możliwych uszkodzeń (u), reprezentowanych przez cechy stanu odwzorowujące rozwijające się uszkodzenia w zintegrowanym systemie biometrycznym. Z drugiej strony z pomiarów otrzymujemy zestaw symptomów (S_m), charakterystycznych dla stanu rozwoju uszkodzeń w chwili pomiaru symptomów.



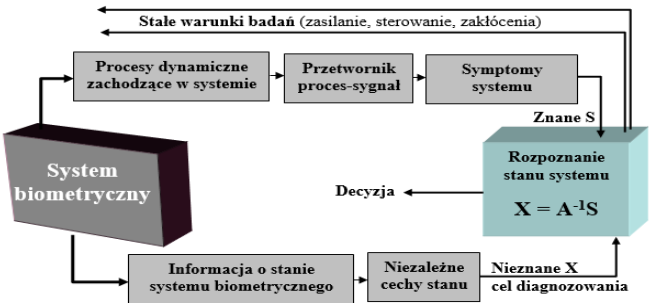
Rys. 8. Obserwacja stanu systemu X za pomocą symptomów S [źródło: opracowanie własne]

Symptomy S_m / Cechy stanu obiektu X_n	Wartości mierzonych symptomów						
	Uz	U_{imp}	I_{zas}	...	K_{wzm}	...	m
1. Napięcie zasilania							
2. Prąd pobierany w stanie czuwania systemu							
3. Czas trwania sprawdzenia toru akustycznego systemu							
.....							
n. Liczba godzin pracy systemu							

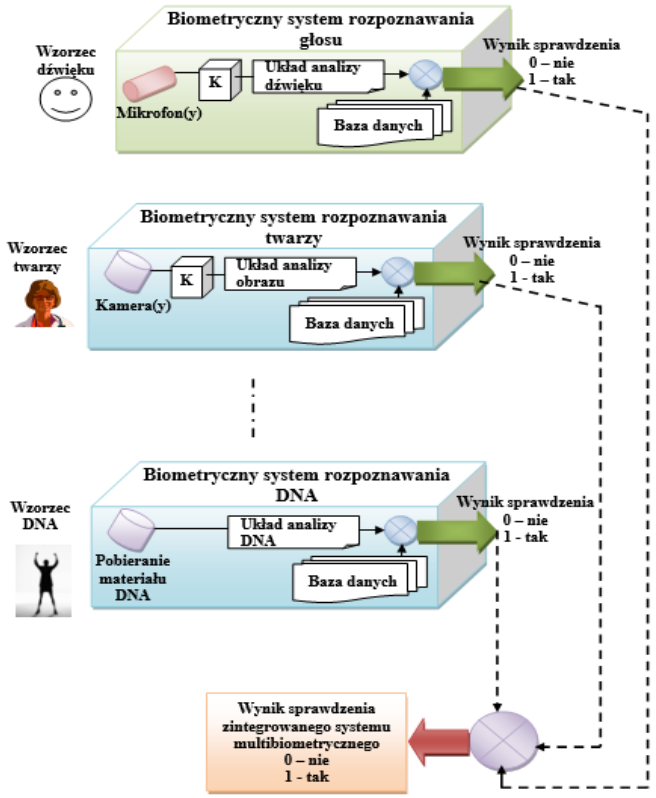
Symptomy diagnostyczne w dziedzinie czasu, częstotliwości, amplitud,... (wymiarowe, bezwymiarowe)

Rys. 9. Tablica obserwacji symptomów S_m dla wybranych cech stanu systemu X_n [źródło: opracowanie własne]

O jednym uszkodzeniu może informować wiele symptomów, przy czym rozwiązanie problemu diagnostycznego wymaga spełnienia warunku $\mathbf{m \geq n}$. Operator systemu biometrycznego wiążący cechy stanu systemu X i jego symptomy S po zidentyfikowaniu, pozwala na bazie pomierzonych symptomów S wnioskować o stanie X [7,10,13]. Tak realizowane zadanie diagnostyczne można przedstawić w postaci systemu jak na rys. 10. Na rys. 11 przedstawiono stanowisko diagnozowania zintegrowanego systemu multibiometrycznego.



Rys. 10. Kolejność postępowania podczas diagnozowania systemu biometrycznego [źródło: opracowanie własne]



Rys. 11. Stanowisko diagnozowania zintegrowanego systemu multibiometrycznego – przykład rozwiązania [źródło: opracowanie własne]

Podsumowanie

W artykule zaprezentowano zagadnienia dotyczące procesu diagnozowania zintegrowanego systemu multibiometrycznego. Wykorzystując system multibiometryczny do procesu identyfikacji osób na rozległym terenie transportowym należy określić wyniki sprawdzeń dla wszystkich torów które wykorzystują różne techniki biometryczne – rys. 11. Wynik sprawdzenia całego systemu multibiometrycznego jest zależny od cząstkowych sprawdzeń wszystkich kanałów – tj. np. dźwięku, twarzy i DNA. Ze względu na wykorzystanie systemu w obiektach transportowych, to jest często w obiektach o tzw. infrastrukturze krytycznej wynik sprawdzenia 1 oznacza sprawne wszystkie w/w podsystemy. Pobieranie, przechowywanie, przetwarzanie i udostępnianie danych biometrycznych regulują dosyć restrykcyjne ustawy i rozporządzenia prawnie. Przestrzeganie przepisów w tej materii w Polsce jest nadzorowane przez Głównego Inspektora Danych Osobowych (GIODO) oraz nowe rozporządzenia i ustawy wynikające z tzw. RODO [1,14].

Bibliografia:

1. Dąbrowski T., Paś J., Olchowik W., Rosiński A., Wiśnios M., Podstawy eksploatacji systemów. Laboratorium, Wojskowa Akademia Techniczna, Warszawa 2014.
2. Dyduch J., Paś J., Rosiński A., Podstawy eksploatacji transportowych systemów elektronicznych, Wydawnictwo Politechniki Radomskiej, Radom 2011.
3. Migdalski J., Inżynieria niezawodności – poradnik, ATR Bydgoszcz 1992.
4. Łubkowski P., Laskowski D., Selected issues of reliable identification of object in transport systems using video monitoring services, in: „Communication in Computer and Information Science", editor: J. Mikulski, vol. 471. Springer, Berlin Hedelberg 2015, pp. 59-68.
5. Łukasiak J., Rosiński A., Analysis of exploitation process in the aspect of readiness of electronic protection systems, "Diagnostyka", 2017, vol. 18, no. 4, pp. 37-42.
6. Paś J., Eksploatacja elektronicznych systemów transportowych, Uniwersytet Technologiczno - Humanistyczny, Radom, 2015.
7. Niziński S., Eksploatacja obiektów technicznych, Wydawnictwo Instytutu Technologii Eksploatacji, Radom 2002.
8. Paś J., Rosiński A., Wiśnios M., Majda-Zdancewicz E., Łukasiak J., Elektroniczne systemy bezpieczeństwa. Wprowadzenie do laboratorium, Wojskowa Akademia Techniczna, Warszawa 2018.
9. Paś J., Rosiński A., Selected issues regarding the reliability-operational assessment of electronic transport systems with regard to electromagnetic interference, "Eksploatacja i Niezawodnosc – Maintenance and Reliability", 2017, 19(3), pp. 375–381, DOI: 10.17531/ein.2017.3.8.
10. Paś J., Shock a disposable time in electronic security systems, „Journal of KONBiN", 2016, nr 2(38).
11. Żółtowski B., Podstawy diagnostyki maszyn, Akademia Techniczno-Rolnicza w Bydgoszczy, Bydgoszcz 1996.
12. Paś J., Siergiejczyk M., Interference impact on the electronic safety system with a parallel structure, „Diagnostyka", 2016, vol. 17, no. 1.
13. Rosiński A., Modelowanie procesu eksploatacji systemów telematyki transportu, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2015.
14. Paś J., Wspomaganie komputerowe procesu eksploatacji systemów bezpieczeństwa, „Biuletyn WAT", 2(666) 2012 Vol. LXI.
15. Siergiejczyk M., Paś J., Rosiński A., Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference, "IET Intelligent Transport Systems", 2016, vol. 10, issue 9, pp. 587–593.
16. Białek K., Paś J.: Exploitation of selected railway equipment - conducted disturbance emission examination, "Diagnostyka", 2018, Vol. 19, No. 3.

Diagnostic station for a multibiometric system for a selected transport object

Multibiometric systems used in transport objects, in contradistinction to "ordinary" biometric systems, use several recognition techniques, e.g. fingerprint, iris, voice or face. Biometric devices are sometimes part of electronic security systems. These systems are currently installed in many transport facilities - stationary and non-stationary where there is a lot of personal traffic. These devices are most often used in extensive areas, airports, logistics bases or railway stations. The article presents issues concerning the diagnostic position for a biometric system which has in its structure several simple identification techniques.

Keywords: biometrics, operation, diagnostics, diagnosis techniques, fingerprint.

Autor:

prof. ndzw. dr hab. inż. **Jacek Paś** – Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Wydział Elektroniki, Instytut Systemów Elektronicznych, Zakład Eksploatacji Systemów Elektronicznych, 00-908 Warszawa, ul. gen. Witolda Urbanowicza 2, jacek.pas@wat.edu.pl