

Zastosowania biometrii – przegląd kluczowych programów i rozwiązań w zakresie ochrony państwa



W ostatnich latach wśród wielu zastosowań biometrii na pierwsze miejsce wysunęło się wspomaganie kontroli granicznej powiązane mniej lub bardziej ściśle z potrzebą skutecznego przeciwdziałania potencjalnie istniejącemu zagrożeniu terrorystycznemu. W celu przedstawienia stanu rzeczy autorzy dokonali przeglądu najistotniejszych projektów biometrycznych wdrażanych obecnie na świecie w obszarze bezpieczeństwa państwa.

Stany Zjednoczone Ameryki Północnej

Po zamachu na budynki World Trade Center w 2001 roku Stany Zjednoczone stały się jednym z niekwestionowanych liderów we wprowadzaniu technologii biometrycznych w ramach ochrony granic państwowych oraz na potrzeby organów ścigania, postrzegając je przede wszystkim jako efektywne narzędzie prewencji i minimalizacji zagrożenia terrorystycznego. Fundamentem legislacyjnym powszechnego stosowania przez agendy federalne danych biometrycznych dla celów identyfikacji osób i weryfikacji ich tożsamości stały się trzy zasadnicze akty prawne:

- USA Patriot Act z 24 października 2001 (ustawodawstwo antyterrorystyczne);
- Aviation and Transportation Security Act z 10 listopada 2001 (ustawodawstwo w zakresie bezpieczeństwa lotnictwa cywilnego i transportu);
- Enhanced Border Security and Visa Entry Reform Act of 2002 z 14 maja 2002 (ustawodaw-

stwo w zakresie bezpieczeństwa granic i reformy wizowej).

Zawarte w nich regulacje, m.in. udzielenie nowych kompetencji agendom federalnym w zakresie zbierania, przetwarzania i wykorzystywania danych biometrycznych, otworzyły nową erę w zakresie ochrony bezpieczeństwa państwa i jego granic.

W ramach systemu instytucji federalnych główną rolę w zakresie stosowania systemów i aplikacji wykorzystujących dane biometryczne osób odgrywa niewątpliwie funkcjonujący od 2003 roku Departament Bezpieczeństwa Wewnętrznego (Department of Homeland Security – DHS), który obecnie realizuje następujące federalne programy ochrony granic z wykorzystaniem technologii biometrycznych:

- **US-VISIT** – uznawany za najwyższy priorytet działania DHS, kompleksowy program kontroli granicznej, który ma zastosowanie do niemal wszystkich podróżnych odwiedzających USA (nieliczne wyjątki to m.in.: dzieci poniżej 14. roku życia i osoby w podeszłym wieku – powyżej 79. roku życia – oraz podróżni ze specjalnymi kategoriami wiz – np. NATO). W ramach pobierania danych biometrycznych od podróżnych skanowane są odciski obu palców wskazujących oraz wykonywana jest cyfrowa fotografia twarzy. Procedura ta jest często wdrażana jeszcze przed przyjazdem do USA, w ramach procesu wizowego w kraju macierzystym podróżnego. Pozwala to zarówno na sprawdzenie danych biome-

trycznych danej osoby z bazami zawierającymi dane przestępców i osób podejrzewanych o działalność terrorystyczną, jak i na wykorzystanie ich do powtórnej autentyfikacji podróżnego już w ramach kontroli granicznej (porównanie danych pozyskanych w trakcie kontroli z danymi umieszczonymi w bazie). US-VISIT jest programem stosowanym nie tylko w ramach procedur wjazdowych, ale również wyjazdowych – obecnie znajduje się w fazie testów kontroli wyjazdowej na dwunastu największych lotniskach USA oraz w dwóch portach morskich. Partnerem Departamentu Bezpieczeństwa Wewnętrznego w realizacji programu US-VISIT jest Departament Stanu.

- **Visa Waiver Program (VWP)** – w ramach którego określono wymagania dla paszportów biometrycznych podróżnych niepodlegających obowiązkowi wizowemu w USA. Zgodnie z jego ustaleniami wszystkie paszporty osób korzystających z programu VWP wydane po 26 października 2006 roku powinny zawierać zintegrowany układ scałony, umożliwiający rejestrację i odczyt danych posiadacza zawartych w tym dokumencie oraz wybranych danych biometrycznych – np. cyfrowej fotografii twarzy (tzw. e-Passport). Podróżni pochodzący z krajów niepodlegających obowiązkowi wizowemu, lecz legitymujący się paszportami niespełniającymi ww. wymagań, nie mogą już korzystać z programu VWP, zatem

w praktyce podlegają obowiązkowi uzyskania wizy.

- **Registered Traveller (RT)** – inicjatywa, której celem jest zaofiarowanie zweryfikowanym – w ramach stosownych procedur – uczestnikom programu znacznie uproszczonych procedur kontroli bezpieczeństwa (głównie na lotniskach) w zamian za uzyskanie statusu RT, co wiąże się między innymi z dobrowolnym udostępnieniem stosownym władzom własnych danych biometrycznych w rozszerzonym zakresie. Program znajduje się obecnie we wczesnej fazie rozwoju, ma mieć charakter partnerstwa publiczno-prywatnego i być rozwiązaniem quasi-komercyjnym, tj. płatnym dla jego uczestników.

- **Nexus** – program obejmujący podróżnych z Kanady często odwiedzających USA. Jest on eksperymentalnie wdrażany na lotnisku w Vancouver, gdzie jego uczestnicy, korzystając ze zautomatyzowanych kiosków, dokonują weryfikacji swojej tożsamości biometrycznej m.in. z użyciem obrazu tęczówki oka.

Należy także – ze względów poznawczych – wspomnieć o kontrolerskim programie biometrycznym realizowanym w latach 2002–2004 przez Departament Bezpieczeństwa Wewnętrznego – tzw. NSEERS (System Rejestracji Wjazd–Wyjazd Bezpieczeństwa Narodowego). Składał się on z dwóch elementów: rejestracji punktu wjazdu i rejestracji krajowej. W obu przypadkach od osób podlegających NSEERS pobierane były dane biometryczne – odciski palców i zdjęcie twarzy – dodatkowo osoby te podlegały przesłuchaniu. Ponadto mogły one wjeżdżać i wyjeżdżać z USA tylko przez określone, wyznaczone im punkty graniczne. Rejestracji punktu wjazdu podlegali co do zasady obywatele pięciu krajów arabskich – Iraku, Iranu, Libii, Sudanu i Syrii. Władze imigracyjne mogły jednak rozszerzyć indywidualnie stosowanie programu na obywatela każdego

państwa obcego wjeżdżającego do USA po 10 września 2002 r. Z kolei część obywateli (mężczyźni w wieku powyżej 16 lat legitymujący się niektórymi rodzajami wiz) wybranych krajów świata – w praktyce z małymi wyjątkami krajów arabskich – przebywających w Stanach Zjednoczonych przed tą datą, a zatem niepodlegających po przybyciu do USA obowiązkowemu pobraniu danych biometrycznych, została objęta drugim elementem NSEERS – rejestracją krajową. Podzieleni na cztery grupy według przynależności narodowościowej, zostali zobowiązani do osobistego zgłaszania się do władz imigracyjnych USA w celu pobrania danych i poddania przesłuchaniu. Do połowy 2003 roku rejestracji w NSEERS dokonało ponad 85 000 osób, z których ponad 13 000 zostało ostatecznie deportowanych. Program ten spotkał się z rozległą krytyką, zwracano uwagę na fakt, że może on być postrzegany jako forma dyskryminacji niektórych grup etnicznych czy religijnych. Warto też podkreślić, że jakkolwiek NSEERS został technicznie zakończony i zastąpiony przez US-VISIT, to Departamentowi Bezpieczeństwa Narodowego pozostawiono kompetencje do wezwania w każdym czasie każdej osoby w nim zarejestrowanej w celu przeprowadzenia dalszych przesłuchań.

Dla stworzenia pełnego obrazu sytuacji należy przedstawić pokrótce także inne istotne programy realizowane aktualnie przez różne agendy rządu federalnego USA, które wiążą się z problematyką biometrii wykorzystywanej dla celów ochrony granic lub innych, związanych z potrzebami wszelkiego rodzaju organów ścigania i sił zbrojnych Stanów Zjednoczonych. Należy do nich zaliczyć:

- Programy badawcze Narodowego Instytutu Standaryzacji i Technologii (NIST – agenda Departamentu Handlu) – realizowane w zakresie technicznych aspektów weryfikacji tożsamości i identyfikacji osób za pomocą takich danych biometrycznych, jak: zdjęcie twarzy, odciski palców i obraz tęczówki oka. NIST wypracowuje

standardy techniczne i rekomendacje, które następnie implementowane są w różnego rodzaju systemach informacji kryminalnej zawierających dane biometryczne, wykorzystywanych przez kompetentne organy. Można zatem przyjąć, że NIST tworzy techniczne podstawy biometrii stosowanej przez agendy federalne.

- Programy Departamentu Obrony – w tym przede wszystkim ABIS (Automated Biometrics Identification System), który w istocie stanowi bazę danych wraz z narzędziami programowymi i aplikacjami dostępowymi. Ich zadaniem jest zbieranie, przechowywanie i inteligentne, wieloaspektowe wyszukiwanie oraz kojarzenie różnego rodzaju danych biometrycznych osób, które znalazły się w kręgu zainteresowania organów stojących na straży bezpieczeństwa narodowego. W początkowej fazie rozwoju ABIS wspiera funkcjonalności oferowane przez odpowiadający mu system Federalnego Biura Śledczego IAFIS (Integrated Automated Fingerprint Identification System) – znajdują się one zresztą w tej samej lokalizacji i zbudowane są w oparciu o tę samą architekturę systemową. Z czasem system będzie rozszerzony o kolejne zaawansowane funkcje biometryczne – m.in. identyfikację obrazu tęczówki. Warto także wspomnieć, że w ramach Departamentu Obrony funkcjonuje Biometrics Fusion Center (BFC – Centrum Fuzji Biometrycznych) – wyspecjalizowana jednostka badawczo-rozwojowa, której zadaniem jest m.in. testowanie i ewaluacja najnowszych komercyjnych technologii związanych z biometrią, a także ich wdrażanie na potrzeby jednostek podległych Departamentowi Obrony.

- Programy Departamentu Sprawiedliwości – to przede wszystkim wspomniany już powyżej IAFIS wykorzystywany przez Federalne Biuro Śledcze do zautomatyzowanego porównywania odcisków palców, a także program NGI (Next Generation Identification – Identyfikacja Nowej Generacji), w istocie funkcjonalne

rozszerzenie IAFIS, którego podstawowym zadaniem jest redukcja aktywności kryminalnej i terrorystycznej za pomocą stosowania w procesie wykrywczym zaawansowanych narzędzi identyfikacji biometrycznej o rozszerzonym zakresie i nowoczesnych technik informacji kryminalnej.

- Programy Departamentu Stanu – poza opisanym już wcześniej uczestnictwem w programie US-VISIT, Departament Stanu odpowiada za wdrożenie paszportu biometrycznego, który po intensywnych przygotowaniach został ostatecznie wprowadzony do produkcji w drugiej połowie 2006 roku. Amerykański paszport biometryczny jest wydawany obywatelom od sierpnia 2006 i spełnia na zasadach wzajemności wymagania stawiane w programie WVP paszportom biometrycznym z krajów obcych (zakodowane dane z ostatniej strony paszportu oraz zdjęcie cyfrowe jego posiadacza).

Australia

Australia wyrosła w ostatnich latach na światowego lidera stosowania dla potrzeb ochrony państwa rozwiązań opartych na danych biometrycznych. Podstawy legislacyjne w tej materii tworzą dwa zasadnicze akty prawne:

- Nowelizacja ustawy imigracyjnej (Migration Act of 1958) z 2004 roku, obowiązująca od 27 sierpnia 2004, która stworzyła prawne podstawy do pobierania danych biometrycznych i rozszerzyła istotnie kompetencje Departamentu Imigracji i Spraw Wielokulturowych w zakresie weryfikacji tożsamości imigrantów na różnych etapach procesu imigracyjnego. Nowelizacja ta zawiera również regulacje zabezpieczające prawo do prywatności w związku z pobieraniem danych biometrycznych oraz określa zasady przechowywania i udostępniania tych danych;

- Ustawa paszportowa z 2005 roku (Passport Act of 2005), obowiązująca od 1 lipca 2005 roku, tworząca prawne podstawy automatyzacji ochrony granic państwowych i wprowadzająca australijski paszport bio-

metryczny. Warto podkreślić, że Australia wprowadziła powszechnie paszporty biometryczne już w październiku 2005 roku, wyprzedzając w tej mierze tak Stany Zjednoczone, jak i kraje Unii Europejskiej, zaś samo rozwiązanie technologiczno-organizacyjne w tej mierze uważane jest za wzorcowe.

Australia jest również krajem, który można stawiać za wzór w zakresie instytucjonalno-organizacyjnego aspektu wykorzystywania danych biometrycznych dla celów ochrony państwa. Problematyka ta jest objęta tzw. zintegrowanym podejściem wyznaczonych organów administracji rządowej – oprócz wspomnianego już Departamentu Imigracji i Spraw Wielokulturowych (DIMA) udział bierze w nim także Departament Spraw Zagranicznych i Handlu (DFAT) oraz Australijska Służba Celna (Customs). W ramach zintegrowanego podejścia DIMA zajmuje się tworzeniem Repozytorium Identyfikacyjnego (Identification Services Repository – ISR), które ma być jednolitym systemem zawierającym wszelkie dane identyfikacyjne, w tym dane biometryczne, pozyskane od obywateli państw obcych w toku procesu wizowego oraz w toku czynności wjazdu na terytorium Australii. Warto podkreślić, że w ramach realizowanego w ISR programu biometrycznego kładzie się nacisk na implementację systemów biometrycznych także w ośrodkach, do których kierowani są po ujawnieniu nielegalni imigranci.

W ramach rozwijania systemu zautomatyzowanej ochrony granic już od 2002 roku na kluczowych lotniskach międzynarodowych Australii testowany jest interesujący system weryfikacji tożsamości o nazwie SmartGate. Jest to rozwiązanie firmy SAGEM Australasia, oparte organizacyjnie na tzw. kioskach SmartGate, w których podróżny może dokonać weryfikacji swojej tożsamości za pomocą porównania cyfrowego zdjęcia twarzy z danymi (również cyfrowe zdjęcie twarzy) przechowywanymi w australijskim paszporcie biometrycznym (ryc. 1). W chwili obecnej nie nastąpiło jesz-

cze powszechne wdrożenie ww. systemu na wszystkich lotniskach międzynarodowych Australii (trwa przedłużona faza testowa dla limitowanej liczby podróżnych i załóg linii lotniczej Qantas, pełne wdrożenie SmartGate przewidywane jest w bieżącym roku), niemniej wieloletnie testy i doświadczenia pozwoliły na uznanie tego rozwiązania za zdecydowany sukces. Podnosi się, że dzięki SmartGate:

- zwiększyła się efektywność ochrony granic;
- zmniejszyło się nasilenie zjawisk posługiwania się sfałszowanymi lub skradzionymi paszportami;
- zwiększyła się przepustowość przejść granicznych;
- wzrosła wygoda pasażerów związana z autoweryfikacją tożsamości.

Chile

Bardzo interesujące rozwiązanie pilotowe w zakresie automatycznej ochrony granic wprowadzono w 2004 roku na lotnisku w Santiago w Chile. Motorem jego zastosowania była – podobnie jak w innych krajach – potrzeba skuteczniejszej ochrony granic w związku z rosnącym zagrożeniem terrorystycznym. Organizacyjne za wdrożeniem tego przedsięwzięcia stoi Policja Investigaciones de Chile (PICH). Chilijski system kontroli biometrycznej to kombinacja skonsolidowanych systemów rozpoznawania zdjęcia twarzy, weryfikacji autentyczności dokumentów podróżnych oraz odcisków palców, zorganizowanych na zasadach kiosków zarządzanych z jednego centralnego punktu (baza danych). Jego działanie wygląda w ten sposób, że podróżny przekazuje w kiosku swój dokument podróżny (paszport) funkcjonariuszowi granicznemu, który dokonuje jego weryfikacji przez automatyczny czytnik, połączony w czasie rzeczywistym ze stosowną bazą danych osób niepożądanych. W tym samym czasie wykonywane jest cyfrowe zdjęcie twarzy pasażera, które porównywane jest z bazą fotografii osób niepożąda-

nych, w tym osób podejrzanych o terroryzm, przestępczość międzynarodową itp., oraz równolegle z danymi zawartymi w sprawdzanym dokumencie podróжным (paszport biometryczny – zdjęcie twarzy posiadacza). Dodatkowo istnieje funkcja pobrania skanów odcisków palców. W wyniku testów systemu ustalono, że cała opisana tu procedura zajmuje w praktyce nie więcej niż 30 sekund (bez daktyloskopowania) – wobec postawionego oryginalnie wymagania 45 sekund na obsługę jednego podróżnego. W związku z sukcesem fazy testowej PICH zamierza stopniowo wdrożyć przedstawiony tu system na większej liczbie przejść granicznych Chile – tak lotniczych, jak i lądowych.

Unia Europejska

Inicjatywy Unii Europejskiej w zakresie wdrażania systemów biometrycznych zostały już przybliżone w artykule pt.: „Biometria – zarys problematyki”, który ukazał się w 254 numerze „Problemów Kryminalistyki”. Dlatego też autorzy skoncentrowali się w tym miejscu głównie na technicznych rozwiązaniach w zakresie paszportu biometrycznego funkcjonującego w krajach członkowskich Unii. Należy przy tym podkreślić, że paszporty te nie zostały wprowadzone w UE w sposób skoordynowany, a inicjatywę w tym zakresie pozostawiono poszczególnym członkom. Za stanowiącą swisty wyznacznik dla działań krajów członkowskich, najogólniejszą regulację wspólnotową w zakresie umieszczania identyfikatorów biometrycznych w dokumentach należy uznać Rozporządzenie Rady WE 15139/04 w sprawie standardów zabezpieczeń i identyfikatorów biometrycznych w paszportach obywateli Unii Europejskiej.

Warto także wspomnieć o kluczowych europejskich programach automatycznej kontroli granicznej, wdrażanych w ostatnich latach przez niektóre kraje Unii, głównie na centralnych lotniskach międzykontynentalnych. Są to przede wszystkim:

- testowany już od 2001 roku na lotnisku Schiphol w Amsterdamzie pierwszy europejski system identyfikacji biometrycznej w oparciu o obraz tęczówki oka – aktualnie rozwijany i dostępny dla członków specjalnie w tym celu stworzonego programu Privium. Celem programu jest m.in. praktyczna weryfikacja działania automatycznego systemu identyfikacji biometrycznej w warunkach dużego przepływu pasażerów.
- realizowany od 2004 roku na lotnisku we Frankfurcie nad Menem program biometrycznej identyfikacji tęczówki oka – będący częścią tzw. inicjatywy ABG (Automated and Biometrics-based Border Checks), skupiającej 18 krajów europejskich – i prowadzony pod auspicjami niemieckiego Federalnego Ministerstwa Spraw Wewnętrznych i Federalnej Straży Granicznej. System był testowany na wybranej grupie pasażerów, którzy wyrazili zgodę na pobranie danych biometrycznych i wprowadzenie ich do bazy;
- rozpoczęta w 2004 roku seria projektów brytyjskich (Projekt Iris – rozpoczęty na lotnisku Heathrow i rozszerzany na inne porty lotnicze Wielkiej Brytanii; Projekt Semafor) będących de facto pierwszą fazą wdrażania pod auspicjami Ministerstwa Spraw Wewnętrznych Wielkiej Brytanii najbardziej chyba kompleksowego w krajach UE programu ochrony granic z wykorzystaniem danych biometrycznych znanego jako e-Borders (ma on funkcjonować w pełni od 2014 roku).

Jeżeli chodzi o krajowe rozwiązania prawne w zakresie paszportów biometrycznych, to aktem o zasadniczym znaczeniu dla ich wprowadzenia jest ustawa z dnia 13 lipca 2006 roku o dokumentach paszportowych (DzU z 2006 r. Nr 143, poz. 1027). Zgodnie z dyspozycją art. 2 ustawy, za dane biometryczne uznano wizerunek twarzy i odciski palców umiesz-

czone w dokumentach paszportowych w formie elektronicznej. Trzeba jednak zwrócić uwagę, że obecnie na podstawie przepisów rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 24 sierpnia 2006 r. w sprawie dokumentów paszportowych oraz trybu postępowania w przypadku ujawnienia fałszerstw lub wad w tych dokumentach oraz w sytuacji ich zniszczenia (DzU z 2006 r. Nr 152, poz. 1090), w zakresie danych biometrycznych, od osób składających wnioski paszportowe wymagane jest jedynie dostarczenie zdjęcia twarzy sporządzonego według ściśle określonej formy.

Wnioski

Przedstawiony w niniejszym artykule ogólniowski przegląd najważniejszych programów służących do realizacji zadań ochrony państwa z wykorzystaniem elementów biometrii pozwala na refleksję w zakresie potrzeb i perspektyw rozwoju oraz realnych warunków ich wykorzystywania.

W pierwszej kolejności należy zwrócić uwagę na asymetrię działań w obrębie Unii Europejskiej. Kraje członkowskie w nieznacznym stopniu realizują je w sposób skoordynowany w oparciu o zalecenia wspólnotowe. Wypada zauważyć, że dokonano jedynie pierwszego kroku, wprowadzając paszporty biometryczne w oparciu tylko o zdjęcia twarzy posiadaczy. Wdrożenie identyfikacji biometrycznej na podstawie tęczówki oka nie wyszło w praktyce poza fazę programów pilotażowych lub adresowanych do zamkniętych grup osób (przykład Holandii). W związku z powyższym kluczową kwestią pozostaje unifikacja działań członków UE, której celem powinno być opracowanie spójnego i efektywnego programu ochrony granic unijnych. Odnosząc się do regulacji krajowych związanych z paszportem biometrycznym, wydaje się, że wykorzystanie daktyloskopii do celów identyfikacji biometrycznej może nie znaleźć szerszego zastosowania, szczególnie w konfrontacji z testo-

wanymi w krajach „starej” Unii rozwiązaniami stawiającymi zdecydowanie na identyfikację na podstawie tęczówki oka. Po dokonaniu wyczerpującego przeglądu technologii i projektów z zakresu biometrii wypada wreszcie skonstatować, że na obecnym poziomie wiedzy nie jest w praktyce możliwe włączenie do arsenału środków biometrycznych metod z zakresu genetyki.

Odrębną kwestią, którą należy wnikliwie rozważyć, jest problem ochrony bezpieczeństwa państwa z wykorzystaniem elementów biometrycznych. Związane z tym ograniczenia swobód obywatelskich. Dopiero przeprowadzenie realnej oceny zagrożenia terrorystycznego i masowa analiza informacyjna adresowana do społeczeństwa mogą przyczynić się do akceptacji ewentualnych ograniczeń praw jednostki i powszechnego wprowadzenia metod biometrycznych do arsenału środków ochrony najszerzej rozumianego bezpieczeństwa kraju.

BIBLIOGRAFIA

1. **Gasperson T.:** Linux prepares a Chile reception for terrorists, [w:] „NewsForge” – gazeta Internetowa Linux i Open Source z dnia 1 listopada 2004.

2. **Most C.M.:** Biometrics and Border Control: Beyond US-Visit, [w:] „Digital ID World”, wrzesień/październik 2004, s. 17 i nast.

3. **Krassowski K., Sołtyszewski I.:** Biometria – zarys problematyki [w:] „Problemy Kryminalistyki” 2006, nr 254, s. 39.

Serwisy internetowe:

www.dhs.com – serwis internetowy Departamentu Bezpieczeństwa Wewnętrznego USA

www.dod.com – serwis internetowy Departamentu Obrony USA

www.state.gov – serwis internetowy Departamentu Stanu USA

www.whitehouse.gov – serwis internetowy Białego Domu (Prezydent USA)

www.tsa.gov – serwis internetowy Agencji Bezpieczeństwa Transportu (USA)

www.nist.gov – serwis internetowy Narodowego Instytutu Standaryzacji i Technologii (USA)

www.usdoj.gov – serwis internetowy Departamentu Sprawiedliwości (USA)

www.fbi.gov – serwis internetowy Federalnego Biura Śledczego (USA)

www.immi.gov.au – serwis internetowy Departamentu Imigracji i Spraw Wielokulturowych (Australia)

www.dfat.gov.au – serwis internetowy Departamentu Spraw Zagranicznych i Handlu (Australia)

www.customs.gov.au – serwis internetowy Australijskiej Służby Celnej

www.biometrics.gov – centralny portal internetowy ds. biometrii administracji federalnej USA

www.iris.gov.uk – serwis internetowy programu IRIS pod auspicjami Home Office.

Przywoływane akty prawne zostały wykazane w treści artykułu.

**Wszystkich Czytelników
zainteresowanych Zeszytami Metodycznymi
z dziedziny badań dokumentów
informujemy,
że redakcja planuje wydać dwa zeszyty,
w których m.in. zostaną zamieszczone prace:**

- Techniki i metody fałszowania dokumentów na przykładzie ujawnionego ośrodka fałszerskiego.
- Kody kreskowe – możliwości odczytywania informacji z kodów o zakłóconej strukturze obrazu.
- Komputer w służbie eksperta badań dokumentów.
- Merk – jako graficzny pierwowzór znaku jakości.
- Monotonia sensoryczna i jej wpływ na zakres odchyłań osobniczych w piśmie ręcznym.
- Wpływ rodzaju podłoża na zmienność cech pisma wykonanego wielkimi literami alfabetu.
- Ocena stopnia stabilności cech identyfikacyjnych podpisów składanych na kartach płatniczych.