ĆWIRKO Joanna [1]
ĆWIRKO Robert [2]

Zastosowanie technik biometrycznych w ochronie obiektów logistycznych

Obiekty logistyczne
System kontroli dostępu
Techniki biometryczne

Streszczenie

W każdym obiekcie logistycznym powinno się stosować system kontroli dostępu. Systemy kontroli dostępu mają za zadanie ograniczenie i uporządkowanie ruchu osób (i/lub pojazdów) na danym terenie lub w obiekcie. W opracowaniu przestawiono zastosowanie urządzeń biometrycznych w systemach kontroli dostępu w obiektach logistycznych. Urządzenia biometryczne wykorzystują do rozpoznawania i identyfikacji osób ich cechy fizyczne i behawioralne.

APPLICATION OF THE TECHNIQUES OF BIOMETRIC PROTECTION OF OBJECTS OF LOGISTICS

Abstract

In each object logistics should apply the system of access control. Access control systems are designed to reduce and organize the movement of people (and/or vehicles) on the ground or in the object. In the development of biometric devices are used in access control systems in facilities logistics. Biometrics use to recognize and identify the persons of their physical characteristics and behavioral.

1. WSTĘP

Prawidłowe funkcjonowanie każdego systemu logistycznego (w szczególności magazynowego lub produkcyjnego) związane jest bezpieczeństwem obiektu, a zwłaszcza z zabezpieczeniem obiektu przed kradzieżą. Zwykle, w większości firm, w których nie ma systemów ochrony, kradzieże mają miejsce, co potwierdzają opracowania przedstawiające źródła strat w systemach logistycznych. Do wejścia w obręb magazynu (strefy składowania) powinny być uprawnione tylko wybrane osoby, nawet poszczególni pracownicy magazynowi powinni mieć przypisane dedykowane strefy, w których mogą się poruszać oraz realizować powierzone zadania.

Dotychczas tworzenie stref ograniczonego dostępu w wielu obiektach logistycznych bazowało na klasycznych zabezpieczeniach mechanicznych z ewentualnymi systemami domofonowymi i ochronie fizycznej. Takie rozwiązania są mało efektywne i są coraz częściej zastępowane nowoczesnymi systemami kontroli dostępu.

2. SYSTEMY KONTROLI DOSTĘPU

System kontroli dostępu ma pozwalać na wejście na teren chroniony tylko osobom uprawnionym. Według normy PN-EN-50133-1 [1] w obiektach mogą występować przejścia kontrolowane (miejsca sterowania dostępem) czterech klas rozpoznania (od 0 do 3) odpowiadających poziomom wiarygodności identyfikacji uprawnionych użytkowników. Klasa rozpoznania dla danego przejścia kontrolowanego może się zmieniać w funkcji czasu (godziny, dni tygodnia, itp.). Pozytywną odpowiedzią na rozpoznanie jest przyznanie dostępu i otwarcie przejścia.

System kontroli dostępu zawiera komplet elementów organizacyjnych i interpretacyjnych oraz komplet elementów wyposażenia technicznego niezbędnego do sterowania dostępem. Obecnie, oprócz standardowej kontroli dostępu coraz istotniejszym stają się możliwość powiązania systemu kontroli dostępu z automatyczną rejestracja czasu pracy pracowników.

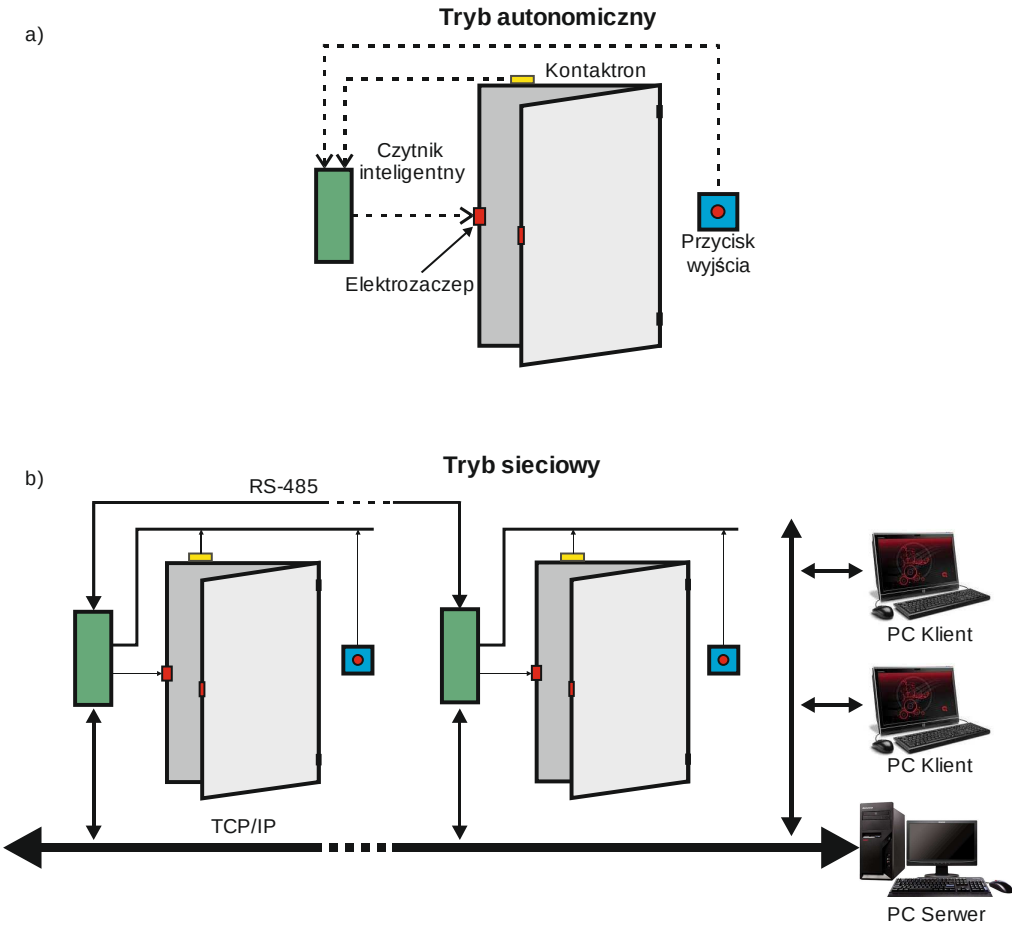
Podstawowymi elementami tworzącymi system kontroli dostępu pod względem funkcjonalnym, organizacyjnym i technicznym są:

- sterownik dostępu (konfiguracje lokalne, nadrzędne, rozproszone pracujące pod kontrolą oprogramowania specjalistycznego);
- czytnik nośnika identyfikacyjnego (np. czytniki kart magnetycznych, Wieganda, zbliżeniowe, terminale z czujnikami cech biometrycznych itp.);
- mechaniczne urządzenie blokujące (np. zamki elektromagnetyczne i elektromotoryczne);
- specjalistyczne oprogramowanie systemu (dla konfiguracji zamkniętych i otwartych z możliwością dołączenia oprogramowania zarządzającego).

[1]Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, Polska 00-908 Warszawa; gen. S. Kaliskiego 2.Tel: +48 22 6839-626, E-mail: joanna.cwirko@wat.edu.pl
[2] Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, Polska; 00-908 Warszawa; gen. S. Kaliskiego 2.Tel: +48 22 6837-123, E-mail: robert.cwirko@wat.edu.pl

Poszczególne funkcje systemu kontroli dostępu mogą być rozproszone pomiędzy większą ilością elementów systemu lub mogą być zintegrowane w jednej obudowie zawierającej kompletny zestaw funkcjonalny np. zamek elektromotoryczny z czytnikiem linii papilarnych.

Systemy kontroli dostępu mogą być realizowane jako zestawy autonomiczne (do obsługi skojarzonego z nimi przejścia, z opcją możliwości zapisu zdarzeń). Mogą też tworzyć zestawy systemów do obsługi wielu przejść np. systemy wielodostępne z kontrolerami nadrzędnymi lub o strukturze rozproszonej, połączonymi siecią własną (np. RS485) lub siecią typu Ethernet (rys. 1).



Rys. 1. Kontrola dostępu – system autonomiczny i system sieciowy

Stopień zabezpieczenia przez system kontroli dostępu zależy od zastosowanej metody identyfikacji/autoryzacji osób. Istnieją trzy podstawowe metody identyfikacji: tokenowe (coś, co masz), metody pamięciowe (coś, co wiesz) lub metody biometryczne (ktoś, kim jesteś).

Metody tokenowe bazują na specjalizowanych, urządzeniach szyfrująco-kodujących lub innych systemach identyfikacyjnych - np. karty identyfikacyjne. Metody te mają dwie zasadnicze wady - po pierwsze, identyfikator może zostać zgubiony, skradziony - po drugie, skopiowany. W obu przypadkach nowy posiadacz otrzymuje dostęp do wszystkich zasobów do których miał dostęp dotychczasowy właściciel, bez żadnych możliwości wykrycia, że nie jest on tym za kogo się podaje.

Metody pamięciowe identyfikują użytkowników przez sprawdzenie ich wiedzy. Najpopularniejsze metody pamięciowe to oczywiście różnego rodzaju hasła. Hasło może zostać zapomniane lub wymuszone np. siłowo lub za pomocą odpowiednich środków farmakologicznych. Jeśli nieautoryzowany użytkownik pozna hasło, nie ma możliwości wykrycia, że nie jest on tym za kogo się podaje.

Metody biometryczne wykorzystują fakt, że pomiar parametrów psychofizycznych człowieka często daje różne wartości dla różnych ludzi. Metody identyfikacji biometrycznej wykorzystują te właściwości, które są charakterystyczne osobniczo.

Najważniejsze cechy identyfikatora biometrycznego to: poziom niezależnego zróżnicowania wybranego wskaźnika w całej populacji ludzkiej, ponieważ od niego zależy wyjątkowość identyfikatora (*indywidualność*); niezmienność identyfikatora w czasie i odporność na wpływy zewnętrzne (*niezniszczalność*); możliwość komputeryzacji procesów kodowania i niezawodnego rozpoznawania wzorca identyfikującego.

Istnieją podstawowe trzy metody wykorzystania identyfikatorów biometrycznych:

- metody statyczne, oparte na identyfikacji odcisków palców, geometrii dłoni; układu naczyń krwionośnych, tęczówki lub siatkówki oka oraz twarzy;

- metody dynamiczne, polegające na rozpoznawaniu pisma ręcznego np. nawyków pisarskich, dynamiki pisania na klawiaturze, głosu np. nawyków mowy i ruchów warg, ruchów ciała;
- metody mieszane (multimodalne) - połączenia w jednym czytniku kilku metod identyfikacyjnych.

W procesach identyfikacji/weryfikacji osoby stosowane są dwa rozwiązania: albo identyfikacja jest dokonywana w samym czytniku (jest to wtedy urządzenie dość złożone) albo w komputerze centralnym do którego podłączone są centrale KD lub inteligentne czytniki.

Czytniki charakteryzujemy przez podanie współczynników: Błędnych Akceptacji – FAR (*ang. False Acceptance Rate)*, Błędnych Odrzuceń – FRR (*ang. False Rejection Rate)* oraz Równości Błędów Akceptacji i Odrzucenia – EER (*ang. Equal Error Rate*)

Współczynnik Błędnych Akceptacji jest określany na podstawie liczby uzyskanych dostępów przez nieuprawnioną osobę. Większa wartość wskaźnika oznacza mniejsze bezpieczeństwo systemu. Im większa jest tolerancja systemu na odchylenia próbki od wzorca, tym większy komfort użytkowników ale i niebezpieczeństwo zaakceptowania użytkowników nieuprawnionych. Współczynnik Błędnych Odrzuceń charakteryzuje poziom liczby osób, które mają prawo uzyskania dostępu, a go nie otrzymują. Im mniejsza tolerancja systemu, tym większe ryzyko, że system odrzuci uprawnionych użytkowników wykazujących odchylenia od zapisanego wzorca.

3. SYSTEMY BIOMETRYCZNE W OBIEKTACH LOGISTYCZNYCH

Najpopularniejsze obecnie systemy biometryczne stosowane w kontroli dostępu wykorzystują następujące cechy fizyczne osób: linie papilarne, geometria dłoni, geometria twarzy, geometria uszu, wzór tęczówki oka, wzór siatkówki oka, weryfikacja podpisu odręcznego. Cechę (biometryczną) powinna charakteryzować akceptowalność w danym środowisku ze względów społecznych, kulturowych i zdrowotnych.

Wprowadzenie systemu kontroli dostępu zwykle nie spotyka się z entuzjazmem pracowników. Jeszcze większy opór jest w wypadku zintegrowania systemu kontroli dostępu z systemem rejestracji czasu pracy. Największe niezadowolenie powoduje wprowadzenie systemów identyfikacji biometrycznej. Jest to związane z praktycznie brakiem możliwości „oszukania" czytnika biometrycznego przez szeregowego pracownika.

W naszych warunkach należy przyjąć, że w obiektach takich jak logistyczne, praktycznie należy stosować głównie czytniki linii papilarnych. Wynika to z kompromisu między kosztami a spodziewanymi efektami. Przykładowo czytniki tęczówki oka zwykle mają niższy poziom błędnych akceptacji niż czytniki linii papilarnych – czyli zapewniają większe bezpieczeństwo, ale są znacznie droższe i trudniejsze w codziennym używaniu.

Z powyższych względów w dalszej części artykułu skupiono się na identyfikacji/weryfikacji opartej o linie papilarne

Szacuje się, że prawdopodobieństwo znalezienia dwóch osób o takim samym kształcie linii papilarnych wynosi około 1 : 64 miliardów. Układ charakterystycznych punktów lini papilarnych – tzw. *minuncji* stanowi podstawę identyfikacji. Czytniki linii papilarnych wyposażone są w okienko, do którego należy przyłożyć opuszkę palca.

Obraz odcisku palca bezpośrednio z czytnika, często jest dość słabej jakości. Pierwszym krokiem jest więc kadrowanie odczytanego obrazu celem odseparowania tła, poprawienie i przetworzenie w celu uzyskania wysokokontrastowego obrazu binarnego Na tak przygotowanym obrazie wyszukiwane są krawędzie (grzbiety linii papilarnych) do których stycznie dodaje się serię krótkich wektorów. Na podstawie obrazu wektorowego specjalny algorytm wyszukuje obszary charakterystyczne (minuncje). Następny etap, to binaryzacja, gdzie za pomocą obrazu o 256 stopniach szarości i stworzonej wcześniej siatki wektorów tworzony jest obraz charakterystyczny linii papilarnych Układ punktów charakterystycznych określony przez wektory zapamiętywany jest jako wzorzec dla palca danej osoby. Opis odcisku palca ma objętość kilkuset bajtów (tym większą, im dokładniejszy jest pomiar).W procesie weryfikacji, rejestrowany jest obraz tego samego palca i przetwarzany w identyczny sposób. Następnie znaleziony układ minucji porównywany jest z zapamiętanym wzorcem. Ze względu na możliwość różnego ułożenia palca na czytniku, czy różną siłę nacisku, za każdym razem kod tworzony na podstawie odcisku palca jest inny.

Kluczowym elementem systemu biometrycznego jest algorytm pozwalający na porównanie odcisku palca ze wzorcem. Z reguły, na każdym palcu można wyznacza się 30 do 40 punktów charakterystycznych. Jednak w związku ze zmiennością pomiarów zakłada się, że zgodność około 20 punktów charakterystycznych jest wystarczająca żeby potwierdzić tożsamość badanej osoby. Algorytmy analizujące powinny być w stanie przetwarzać obrazy silnie zaburzone (na przykład odcisk brudnego palca) i umieć rozpoznać linie papilarne niezależnie od ułożenia palca na czytniku.

- czujniki pojemnościowe (rys. 2) – rejestrujące pojemność kondensatora utworzonego między elektrodami urządzenia a palcem;
- czujniki optyczne – rejestrujące obraz linii papilarnych (zapis cyfrowy) – rys. 3;
- czujniki termiczne – rejestrujące różnicę temperatur pomiędzy poszczególnymi punktami linii papilarnych;
- czujniki naciskowe - rejestrujące nacisk palca (matryca czujników nacisku).

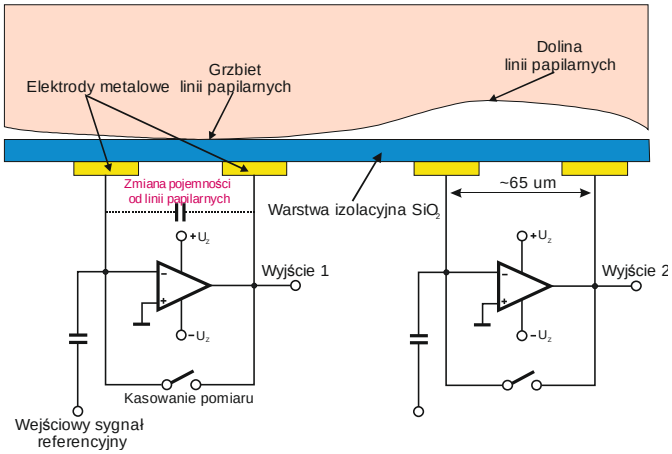
Podstawową funkcją urządzenia biometrycznego w systemie kontroli dostępu jest weryfikacja autentyczności osoby. Kontrola dostępu wymaga jednak nie tylko identyfikacji osoby, lecz również otwierania drzwi, zezwalania na dostęp lub odmawiania go, oraz monitorowania sytuacji alarmowych. Czytniki biometryczne mogą pracować w konfiguracjach jednostanowiskowej oraz systemach zintegrowanych lub sieciowych.

W systemach jednostanowiskowych użytkownicy rejestrowani są w czytniku, gdzie następnie przechowywany jest też ich wzór biometryczny. Podczas weryfikacji, urządzenie porównuje wzór otrzymany z wzorem przechowywanym w pamięci. Liczba użytkowników jest ograniczona przez pamięć urządzenia. Z takim czytnikiem najczęściej zintegrowana jest część wykonawcza pozwalająca np. uruchomić zamek elektromagnetyczny.

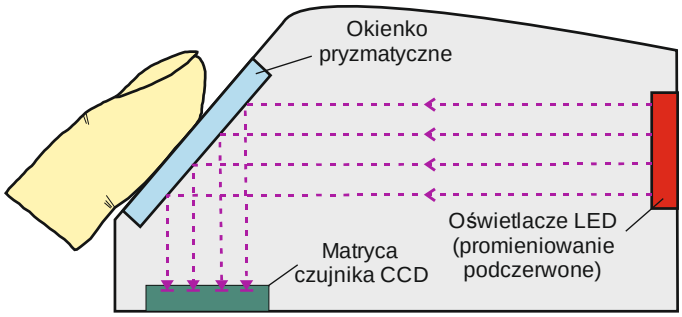
Przy integracji czytników biometrycznych stosuje się dwie główne konfiguracje pracy:

- czytniki połączone w grupy, gdzie jeden z nich pełni role nadrzędną (Master), zaś pozostałe są urządzeniami podrzędnymi (Slave), nie jest w tym przypadku potrzebny dodatkowo komputer;
- czytniki w grupie są nadzorowane przez komputer centralny.

W przypadku czytników inteligentnych, możliwa jest konfiguracja rozproszona, w której czytniki są równoprawne (każdy ma takie same uprawnienia do zarządzania systemem).



Rys. 2. Zasada pracy czujnika pojemnościowego urządzenia biometrycznego



Rys. 3. Zasada pracy czujnika optycznego urządzenia biometrycznego

W pierwszym przypadku główną zaletą jest możliwość wspólnego korzystania z baz danych wzorców poszczególnych czytników i wzajemne ustalanie relacji dostępu. W drugim przypadku uzyskuje się możliwość centralnego monitorowania systemu i efektywnego zarządzania różnymi organizacjami baz danych. W ramach systemu zintegrowanego czytniki połączone są przez różnorodne interfejsy np. RS422, RS485, modem czy sieć komputerową.

W systemach sieciowych działających w oparciu o technologie LAN i WAN każdy czytnik jest jednostką niezależną i zwykle ma wbudowany serwer www. Czytniki tworzą system rozproszony i mogą znajdować się w różnych lokalizacjach geograficznych (miasta, kraje, kontynenty). Administrator systemu może podłączyć się do sieci z dowolnego punktu na świecie przez przeglądarkę internetową.

W zależności od wielkości obiektu należy wybrać właściwe rozwiązanie. Rozwiązania jednostanowiskowe dedykowane są dla obiektów niewielkich. Rozwiązania sieciowe są optymalne dla dużych firm logistycznych, których obiekty znajdują się w wielu lokalizacjach znacznie odległych od siebie.

Przedstawiony na rysunku 4 terminal iGuard LM520 firmy Lucky-Tech [2,3] jest biometrycznym systemem kontroli dostępu i rejestracji czasu pracy wykorzystującym dla identyfikacji odcisku palca technologię DFX (*ang. Difficulty Figerprint Extraction*). Technologia ta jest obecnie najbardziej efektywną technologią dla rejestrowania wzorców biometrycznych większości ludzi i cechuje się bardzo niskim współczynnikiem błędnych odrzuceń. W procesie identyfikacji wykorzystywany jest sensor pojemnościowy analizujący obraz odcisku palca z rozdzielczością 265*300 punktów. Normalnie sensor jest zasłonięty przesuwną przesłona ochronną, która jest odsuwana przy przykładaniu palca. Urządzenie posiada wbudowany serwer www umożliwiający zdalne zarządzanie czytnikiem.

Przy instalacji terminala iGuard w sieci LAN wystarczy przeprowadzić procedurę identyczną do tej jaką wykonuje się przy sieciowej instalacji komputera PC, tj. podanie adresu IP, maski podsieci, domyślnej bramy i opcjonalnie DNS.

Rys. 4. Czytnik biometryczny iGuard firmy Lucky-Tech

Dostęp do terminala może być realizowany z dowolnego systemu operacyjnego przez przeglądarkę internetową. Jest to wygodne dla kierownictwa firmy – z dowolnej lokalizacji można na bieżąco nadzorować pracę firmy. W środowisku sieciowym urządzenia iGuard są konfigurowane w układzie Master/Slave. - jedno z urządzeń pełni rolę nadrzędną w stosunku do pozostałych. Dodatkowo iGuard może komunikować się z urządzeniami zewnętrznymi przez interfejsy RS232, RS485 i Wieganda.

Czytnik linii papilarnych IMMSkan 300 opracowany przez Instytut Maszyn Matematycznych (rys. 5) jest przeznaczony do zastosowań w systemach kontroli dostępu i w systemach rejestracji czasu pracy. Terminal może pracować autonomicznie lub z komputerem [4].

Rys. 5. Czytnik linii papilarnych IMMSkan 300 opracowany przez Instytut Maszyn Matematycznych

Umożliwia rejestrację wzorców linii papilarnych użytkowników, rejestrację zdarzeń o ruchu osób wchodzących i wychodzących, nadawanie i cofanie uprawnień poszczególnym użytkownikom, zmianę parametrów konfiguracyjnych urządzenia. W systemach kontroli dostępu pełni rolę inteligentnego zamka zwalniającego blokadę przejścia tylko dla osób uprawnionych i nadzoruje stan przejścia, sygnalizując próbę jego sforsowania. Informacja o zdarzeniach (przejściach) użytkowników jest wysyłana poprzez interfejs komunikacyjny RS-232/485 lub sieć komputerową do programu zarządzającego systemem. Rozpoznawanie użytkowników odbywa się w terminalu, co znacznie obniża czas oczekiwania na weryfikację.

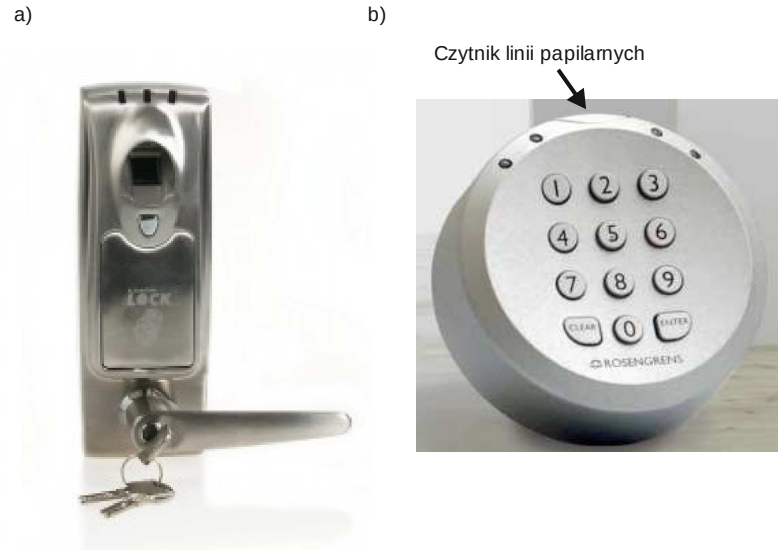
W systemach rejestracji czasu pracy czytnik pracuje pod kontrola programu XChronos i pracownik wybiera z klawiatury czytnika odpowiedni tryb wejścia/wyjścia – jest dziewięć opcji służbowych i prywatnych. Czytnik rejestruje czasy przyjścia oraz wyjścia z pracy z jednoczesnym odnotowaniem ich rodzaju (służbowe, prywatne itd.). Dane te po przekazaniu do komputera centralnego (z systemem XChronos) są podstawą do naliczania przepracowanego czasu i sporządzania indywidualnych raportów miesięcznych.

Czytnik biometryczny BioStation firmy Suprema Inc. przestawiony na rysunku 6 może pracować autonomicznie lub w rozwiązaniach sieciowych rozproszonych [5]. Czytnik Biostation w połączeniu z oprogramowaniem RCP ACCESS NET umożliwia profesjonalną rejestrację i rozliczenia czasu pracy. Oprogramowanie czytnika współpracuje z innymi

komercyjnymi programami rejestracji pracy (możliwość eksportu pliku w odpowiednim formacie). Czytnik jest dedykowany dla dużych firm – ma możliwość przechowywani do 50 000 wzorów odcisków palca i 500 000 zdarzeń w pamięci wewnętrznej.

Rys. 6. System z czytnikiem biometrycznym BioStation firmy Suprema Inc.

W wielu przypadkach nie jest konieczny system kontroli dostępu w ramach całej firmy. Wystarczające jest tylko zabezpieczenie przed osobami niepowołanymi niektórych stref czy pojedynczych pomieszczeń w obiekcie. W takim przypadku dobrym rozwiązaniem jest stosowanie prostych systemów autonomicznych. Jest to zintegrowanie w jednej obudowie kompletnego zestawu funkcjonalnego np. zamka elektromotorycznego z czytnikiem linii papilarnych.
Na rysunku 7 przedstawiono autonomiczne systemy kontroli dostępu w postaci dwóch zamków biometrycznych uruchamianych liniami papilarnymi palca.



Rys. 7. Zamki biometryczne rozpoznające układ linii papilarnych palca: a) AL-K firmy Auraton, b) REL firmy Rosengrens

Pierwszy zamek typu AL-K firmy Auraton Lock [6] jest przeznaczony do zabezpieczeń pomieszczeń mieszkalnych, gospodarczych, laboratoriów, serwerowni, itp. Wyposażony jest w dwa układy kontrolne: czytnik linii papilarnych i klawiaturę do wprowadzenia hasła, aktywowane wspólnie lub rozdzielnie. Można zapisać 99 wzorców linii papilarnych (opcjonalnie 640). Maksymalna długość hasła wynosi 10 cyfr. Przedstawiona wersja zamka pozwala także na awaryjne otworzenie zamka za pomocą patentowego klucza. Możliwa jest aktywacja funkcji „usypiania" powodującej, że po pięciokrotnym kolejnym okazaniu niewłaściwego odcisku palca, czytnik linii papilarnych blokuje się na pięć minut.

Drugi przedstawiony zamek typu REL f-my Rosengrens [7] jest przeznaczony do zabezpieczenia sejfów, drzwi kancelarii tajnych, itp. Przy użyciu klawiatury można, oprócz wprowadzenia haseł typ master i slave, uaktywnić funkcje dodatkowe jak np.: funkcje opóźnienia (od 0 do 99 minut), dodatkowe 5 kodów użytkownika, 1 kod CIT (dla konwojenta) lub otwarcie komisyjne, czyli konieczność wpisania dwóch różnych kodów celem otwarcia zamka. Czytnik linii papilarnych pozwala na zapamiętanie 40 różnych wzorców. Podobnie jak w poprzednim zamku klawiatura i czytnik biometryczny mogą być aktywowane do pracy wspólnej lub rozdzielnej.

4. WNIOSKI

Obiekty logistyczne, a zwłaszcza magazyny i hurtownie stanowią zbiór różnorodnych dóbr materialnych, będących przedmiotem pożądania mniej praworządnych obywateli.
Systemy kontroli dostępu mają za zadanie zarządzanie ruchem osób i pojazdów w oparciu o odpowiednio skonfigurowaną bazę danych oraz archiwizację zdarzeń z tym związanych. Baza danych systemu zawiera między innymi uprawnienia związane z przydzielonym każdemu użytkownikowi dostępem w funkcji czasu do poszczególnych stref obiektu.

W opracowaniu przestawiono zastosowanie urządzeń biometrycznych w systemach kontroli dostępu stosowanych w ochronie obiektów logistycznych. Urządzenia biometryczne wykorzystują do rozpoznawania i identyfikacji osób ich cechy fizyczne i behawioralne. Cechy brane pod uwagę do identyfikacji biometrycznej mają wyjątkowy charakter – są unikalnym identyfikatorem dla każdej osoby – a ponieważ wykazują niezmienność i niezniszczalność, stanowią trudne do podrobienia dane, których teoretycznie nie można ukraść, nie można zgubić i nie trzeba pamiętać.

O zastosowania danej metody biometrycznej w systemach kontroli dostępu decyduje oprócz jej skuteczności także łatwość realizacji technicznej i jej koszt a przede wszystkim prostota użytkowania. Uwzględniając te uwarunkowania autorzy artykułu sugerują stosowanie głównie czytników linii papilarnych w systemach kontroli dostępu stosowanych w ochronie obiektów logistycznych.

5. BIBLIOGRAFIA

[1] *Polska Norma PN-EN 50133-1:2007. Systemy alarmowe – Systemy kontroli dostepu w zastosowaniach dotyczących zabezpieczenia – Część 1. Wymagania systemowe*
[2] *Instrukcja obsługi iGuard Seria LM* firmy Lucky-Tech
[3] *Materiały informacyjne* udostępnione przez firmę Deep Blue Biometrics Sp. z o. o., 00-678 Warszawa, ul. Wilcza 33/5
[4] *Dokumentacja techniczna czytnika IMMSkan 300*
[5] *Dokumentacja techniczna czytnika Biostation*
[6] *Dokumentacja techniczna zamka biometrycznego AL-K* firmy Auraton Lock,
[7] *Dokumentacja techniczna zamka elektronicznego REL* firmy Rosengrens, http://www. rosengrens.com