Analiza niezawodnościowo-eksploatacyjna systemów bezpieczeństwa o nadzorze informatycznym

Waldemar Szulc[1], Adam Rosiński[2]

[1] Wydział Informatyki Stosowanej i Technik Bezpieczeństwa, Wyższa Szkoła Menedżerska w Warszawie
[2] Wydział Transportu, Politechnika Warszawska

Streszczenie: Obserwowany w ostatnich latach rozwój technik biometrycznych umożliwił identyfikowanie osób na podstawie unikalnych cech, jak wielkość i kształt dłoni, odciski palców, głos, oko. Dzięki postępowi w elektronice i technice mikroprocesorowej oraz spadkowi cen, czytniki biometryczne stosuje się już w wielu elektronicznych systemach bezpieczeństwa. W artykule przedstawiono koncepcje wybranych, zintegrowanych elektronicznych systemów bezpieczeństwa do ochrony obiektów o specjalnym przeznaczeniu i nadzorze informatycznym, w których stosowane są m.in. metody biometryczne do identyfikacji osób. Opisano techniki ochrony obiektów rozległych terytorialnie ze szczególnym uwzględnieniem ich specyfiki. Autorzy od lat prowadzą badania niezawodnościowo-eksploatacyjne elektronicznych systemów bezpieczeństwa.

Słowa kluczowe: system bezpieczeństwa, niezawodność, biometria

1. Wprowadzenie

Artykuł jest efektem wieloletnich badań elektronicznych systemów bezpieczeństwa o różnych stopniach złożoności. Badania dotyczą procesów eksploatacyjno-niezawodnościowych rozproszonych systemów bezpieczeństwa, ze szczególnym uwzględnieniem zagrożeń wyższych kategorii, klasyfikowanych jako stopień 3 i stopień 4 (dawne Z3 i Z4). Szczegółowe badania skierowane są na obiekty o znacznym stopniu komplikacji, z uwzględnieniem systemów rozproszonych. Obiekty te są zwykle wyposażone w rozbudowane elektroniczne systemy bezpieczeństwa o charakterze rozproszonym, zawierające systemy monitoringu wizyjnego wysokiej rozdzielczości z rejestracją na dyskach HDD i z możliwością archiwizacji na DVD, systemy kontroli dostępu realizowane niezależnie lub stanowiące fragment centrali i systemy przeciwpożarowe niezależne lub (w ograniczonym zakresie) stanowiące fragment centrali. Autorzy uwzględniają również złożone systemy przeciwpożarowe współpracujące z DSO (Dźwiękowe Systemy Ostrzegania). Zwykle elektroniczne systemy bezpieczeństwa są powiązane z systemami mechanicznymi (drzwi, okna, a w nich klasyfikowane szyby, rygle drzwiowe, trzymaki elektromagnetyczne itp.). Autorzy przedstawiają w postaci grafów relacje zachodzące w elektronicznych systemach bezpieczeństwa. Warto nadmienić, że obiekty o specjalnym przeznaczeniu mogą mieć specjalne czytniki kart, pastylki Dallas, jak również skomplikowane czytniki biometryczne. Biometryczny sposób sterowania złożonym systemem bezpieczeństwa obiektu o specjalnym przeznaczeniu wymaga dużej wiedzy projektantów i potencjalnych wykonawców systemu na temat budowy modelu niezawodnościowo-eksploatacyjnego oraz sposobu określania wskaźników gotowości Kg na podstawie obserwacji, żmudnych badań i analizy uszkodzeń rejestrowanych na specjalnych formularzach.

Autorzy przeprowadzili analizę systemów bezpieczeństwa i opisali je równaniami matematycznymi, pozwalającymi wyznaczyć prawdopodobieństwo przebywania systemu w ściśle określonych stanach eksploatacyjno-niezawodnościowych. Badania praktyczne zaczęto realizować w 2005 r., zbierając dane eksploatacyjno-niezawodnościowe z wielu elektronicznych systemów bezpieczeństwa o skomplikowanej budowie i podobnej konfiguracji (opracowano specjalne karty do zbierania danych o uszkodzeniach). W trakcie zbierania danych o uszkodzeniach autorzy napotykali na szereg problemów eksploatacyjno-niezawodnościowych, szczególnie w systemach rozproszonych zrealizowanych w obiektach o szczególnym przeznaczeniu.

Zintegrowany i rozproszony system bezpieczeństwa został zaprojektowany na bazie jednostki mikroprocesorowej typu INTEGRA 64. Zaproponowano układ blokowy (niezawodnościowy) elektronicznego systemu bezpieczeństwa interpretujący opracowany schemat ideowy, a następnie zbudowano model eksploatacyjno-niezawodnościowy w postaci grafu przejść. W szczegółowych badaniach uwzględniono dane zebrane podczas eksploatacji systemu bezpieczeństwa, także z biometrycznych czytników linii papilarnych. Wykorzystano skomplikowany aparat matematyczny umożliwiający obliczenie prawdopodobieństwa przebywania systemu bezpieczeństwa w określonym stanie eksploatacyjnym (np. przejście ze stanu pełnej zdatności do stanu zagrożenia bezpieczeństwa). Zdefiniowano wniosek: niezawodność rozproszonych systemów bezpieczeństwa należy kształtować już na etapie projektowania, jak również podczas praktycznej realizacji systemu. Niezawodność można również korygować w trakcie eksploatacji poprzez rozbudowę i modernizację już istniejącego systemu lub zmiany w strukturze niezawodnościowej, choć niektóre bloki systemu są na taką korektę odporne.

System pełnej sygnalizacji zagrożeń (tzw. ochrony elektronicznej), w zależności od wykrywanych zagrożeń, tworzą systemy:
- sygnalizacji włamania i napadu
- sygnalizacji pożaru
- kontroli dostępu
- monitoringu wizyjnego
- ochrony terenów zewnętrznych (system obwodowy i peryferyjny).

Ochrona wynikająca z działania tych systemów może być uzupełniona przez systemy:
- sygnalizacji stanu zdrowia lub zagrożenia osobistego,
- sygnalizacji zagrożeń środowiska,
- przeciwkradzieżowe,
- dźwiękowe ostrzegawcze, np. współpraca z systemami przeciwpożarowymi,
- zabezpieczenia samochodów przed włamaniem i uprowadzeniem oraz nawigacji satelitarnej (GPS) i naziemnej radiokomunikacyjnej (np. GSM, GSM-R).

Istotnym elementem systemów alarmowych są systemy transmisji alarmu stanowiące urządzenia albo sieci do przekazywania informacji o stanie jednego lub więcej systemów alarmowych do jednego lub kilku alarmowych centrów odbiorczych wraz z opcjami kryptograficznymi.

2. Biometria i Systemy Kontroli Dostępu

Skomplikowane elektroniczne systemy bezpieczeństwa projektowane i montowane w obiektach o specjalnym przeznaczeniu (np. w kancelariach tajnych) wymagają specjalnych czytników identyfikujących użytkownika. Czytniki biometryczne w systemach kontroli dostępu stosuje się od lat siedemdziesiątych. Początkowo instalowano je w instytucjach wymagających specjalnych zabezpieczeń, głównie ze względu na ich wysoki koszt. Ostatnio koszt czytników biometrycznych zdecydowanie spadł, a ich precyzja działania wzrosła, co pozwoliło na szersze stosowanie wyszukanych czytników biometrycznych. Obecnie już nie tylko obiekty specjalnego przeznaczenia, jak elektrownie jądrowe, lotniska, wytwórnie papierów wartościowych i kancelarie tajne, ale wiele firm może sobie pozwolić na biometryczną kontrolę dostępu, a więc kontrolę przepływu ludzi. Zastosowanie czytników biometrycznych w obiektach specjalnego przeznaczenia to już obligatoryjny wymóg.

Badania niezawodnościowo-eksploatacyjne czytników biometrycznych są skomplikowane ze względu na ich bardzo złożony charakter. Artykuł prezentuje zagadnienia integracji biometrii do zadań kontroli dostępu w aspekcie badań niezawodnościowo-eksploatacyjnych. Celem systemu kontroli dostępu (samodzielnej lub wchodzącej w skład elektronicznego systemu bezpieczeństwa) jest dopuszczenie wyłącznie uprawnionych użytkowników do określonych miejsc w obiekcie. System kontroli dostępu oparty na kartach (wszelkiego typu), bardziej kontroluje dostęp tych kart niż samych użytkowników. Nie jest zatem w pełni bezpieczny. Elektroniczne systemy bezpieczeństwa wyposażone w klawiatury (do wprowadzania kodów PIN) umożliwiają dostęp każdemu, kto zna kod, niezależnie od tego, czy jest to osoba uprawniona, czy nie. Tylko urządzenia z czytnikami biometrycznymi weryfikują faktycznie osobę. Sterowanie biometryczne elektronicznych systemów bezpieczeństwa pozwala wyeliminować m.in. karty magnetyczne. Daje to znaczne oszczędności finansowe i administracyjne oraz upraszcza logistykę. Utrata karty powoduje konieczność wystawienia nowej. Jeśli chodzi o oko (źrenica) albo rękę, to trudno będzie „zgubić" te części ciała człowieka.

Ważną funkcją urządzenia z czytnikiem biometrycznym sterującym elektronicznym systemem bezpieczeństwa jest weryfikacja autentyczności użytkownika. Kontrola dostępu nie tylko ogranicza się do identyfikacji użytkownika, realizuje również otwieranie drzwi, zezwala na dostęp lub odmawia go oraz monitoruje alarmy. Znakomita większość systemów kontroli dostępu nadzoruje więcej niż jedne drzwi (jednostronne lub obustronne). W takiej sytuacji można zastosować kilka systemów pojedynczych, ale częściej stosuje się rozwiązanie sieciowe. Łącząc czytniki biometryczne ze sobą, a następnie z komputerem, otrzymuje się wygodny i łatwy w obsłudze system kontroli dostępu umożliwiający centralne monitorowanie. Tak też jest w omawianym elektronicznym systemie bezpieczeństwa.

Do komputera, który zlokalizowany jest w pomieszczeniach ochrony, przekazywane są sygnały o wszystkich zdarzeniach, tutaj też następuje aktywowanie punktów drzwiowych (sterowanie ryglami, elektrozaczepami, siłownikami magnetycznymi). Wszystkie zdarzenia rejestrowane są w pamięci komputera i mogą być wykorzystane w dowolnym momencie. Komputer przechowuje *wzory biometryczne*, np. linie papilarne palca użytkownika, analizuje układ krwionośny dłoni i źrenicę oka, co umożliwia wprowadzanie danych użytkownika na dowolnym czytniku (system roześle wzory do pozostałych punktów kontrolnych). Usunięcie użytkownika lub zmiana warunków dostępu odbywa się programowo. Pewne systemy biometryczne przechowują wszystkie informacje wyłącznie w pamięci komputera i tam też odbywa się weryfikacja wzoru biometrycznego. Inne systemy rozprowadzają wzory biometryczne do poszczególnych czytników. W ramach sieci czytniki połączone są łączem RS-232, RS-485 lub przez modem, a w systemach głosowych wykorzystuje się linie telefoniczne. Znane są systemy biometryczne analizujące twarz człowieka i jej szczegóły. Elektroniczne systemy bezpieczeństwa sterowane czytnikami biometrycznymi wymagają dużej staranności na etapie projektowania jak również i podczas samej realizacji obiektowej.

Do istotnych składników elektronicznych systemów bezpieczeństwa, w tym systemów kontroli dostępu, należy również zaliczyć:
- akceptację (uwierzytelnienie) użytkownika przez czytnik biometryczny,
- wskaźnik błędnych odrzuceń,
- zrównoważony wskaźnik błędu w urządzeniach z czytnikami biometrycznymi,
- ocenę danych statystycznych z zastosowaniem czytników biometrycznych,
- przepustowość urządzeń z czytnikami biometrycznymi.

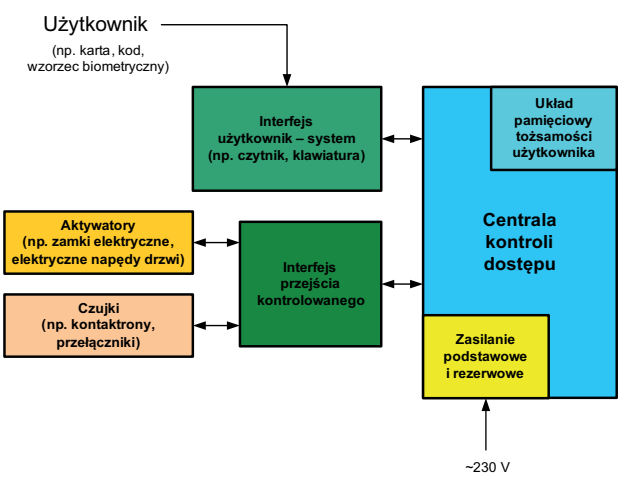
Biometria pozwala na precyzyjną identyfikację użytkowników poprzez wykorzystanie ich niepowtarzalnych charakterystycznych cech. Ważnymi cechami anatomicznymi każdego człowieka są m.in.:
- geometria dłoni (jednej albo obu)
- linie papilarne
- geometria twarzy wraz z charakterystycznymi cechami
- geometria ucha
- geometria ust
- budowa oka (cechy charakterystyczne tęczówki i siatkówki oka)
- układ żył nadgarstka lub naczyń palca
- barwa głosu.

Do cech behawioralnych można zaliczyć m.in. charakterystyki: mowy, ruchu ust, ruchu gałki ocznej, pisma, chodu.

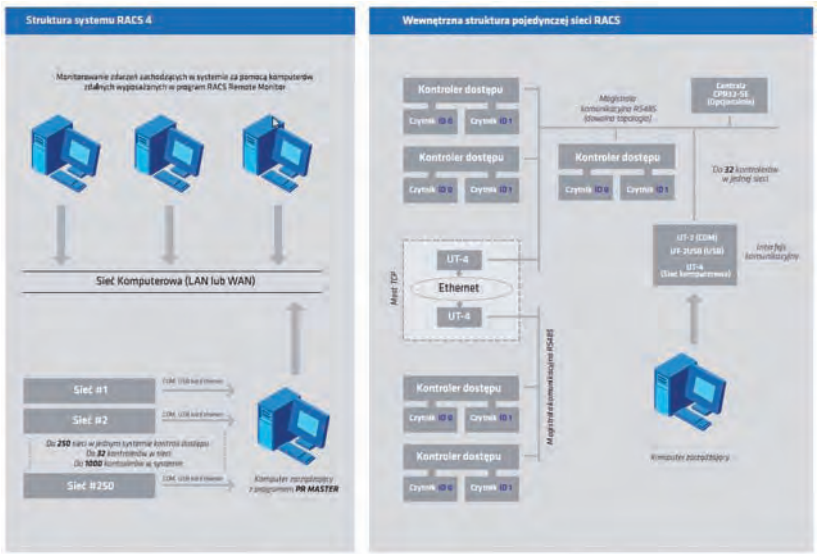
System kontroli dostępu (SKD) to zespół urządzeń i oprogramowania, mający za zadanie:
- identyfikację osób albo pojazdów uprawnionych do przekroczenia granicy obszaru zastrzeżonego oraz umożliwienie im wejścia/wyjścia,
- niedopuszczenie do przejścia granicy obszaru zastrzeżonego przez osoby albo pojazdy nieuprawnione,
- wytworzenie sygnału alarmowego informującego o próbie przejścia osoby albo pojazdu nieuprawnionego przez granicę obszaru zastrzeżonego,
- zarejestrowanie np. numerów rejestracyjnych samochodów.

Na rys. 1 przedstawiono uproszczony schemat blokowy elektronicznego systemu bezpieczeństwa (systemu kontroli dostępu). Użytkownik, aby przejść przez kontrolowane przejście musi potwierdzić swoją tożsamość, np. przykładając kartę zbliżeniową czy podając kod PIN. Interfejs użytkownik-system przesyła odczytane dane do centrali kontroli dostępu, gdzie zostaje ona porównana (wykorzystując m.in. komparator) z wcześniej zapamiętanymi danymi i cechami użytkownika. Jeśli wszystkie dane się zgadzają, to za pośrednictwem interfejsu przejścia kontrolowanego następuje uruchomienie aktywatorów przejścia (np. otwarcie zamka elektrycznego czy włączenie elektrycznego napędu otwarcia drzwi), zwolnienie rygli lub trzymaków magnetycznych. System kontroli dostępu ma także czujki (najczęściej kontaktronowe), które określają, czy drzwi zostały zamknięte po przejściu uprawnionej osoby lub czy nie zostały otwarte w sposób niedozwolony (np. siłowy). W systemie może występować także moduł komunikacji z innymi centralami kontroli dostępu i innymi systemami zarządzania bezpieczeństwem budynku (systemy sygnalizacji włamania i napadu,. systemy przeciwpożarowe, systemy monitoringu wizyjnego itp.).

Przejście kontrolowane zazwyczaj jest wyposażone w:
- czytnik (coraz częściej biometryczny)
- czujki kontaktu
- przycisk otwarcia
- przycisk ewakuacyjnego otwarcia drzwi (wymagania przeciwpożarowe)
- element ryglujący (np. rygiel, zwora magnetyczna, zamek elektromechaniczny)
- samozamykacz (jednofazowy lub dwufazowy)
- pochwyt (pochwyty).



Rys. 1. Uproszczony schemat blokowy systemu kontroli dostępu
Fig. 1. Simplified scheme of control access system



Rys. 2. Schemat blokowy systemu kontroli dostępu RACS 4 firmy ROGER
Fig. 2. Scheme of Control Access System RACS 4 – firm ROGER

Na rys. 2 przedstawiono system kontroli dostępu RACS 4 firmy ROGER. Jest to sieciowy system kontroli dostępu składający się z:
- kontrolerów dostępu serii PR,
- czytników serii PRT,
- modułów rozszerzeń XM-2/XM-8,
- kontrolera sieciowego (centrala) CPR,
- oprogramowania zarządzającego PR Master.

W systemie tym w jednej sieci może funkcjonować do 32 kontrolerów dostępu, które są połączone magistralą komunikacyjną RS-485. Jej maksymalna długość wynosi 1200 m. Cały system może składać się z 250 sieci, przy czym łącznie obsługiwanych jest maksymalnie 1000 kontrolerów. Każda sieć może być połączona z komputerem zarządzającym (z zainstalowanym oprogramowaniem PR Master) za pośrednictwem interfejsu komunikacyjnego przekształcającego RS-485 na COM lub USB lub Ethernet.

3. Integracja z innymi systemami kontroli dostępu

Producenci urządzeń biometrycznych oferują różne sposoby zintegrowania czytników biometrycznych z konwencjonalnymi elektronicznymi systemami bezpieczeństwa. Najczęściej stosowana jest metoda ***emulacji czytnika kart.*** W tym przypadku urządzenie biometryczne współpracuje z systemem w taki sposób jak czytnik kart. ***Wyjście czytnika kart*** w urządzeniu biometrycznym zostaje podłączone do ***portu czytnika*** w panelu sterującym. Metoda ta jest najbardziej efektywna w odniesieniu do systemów opartych na kartach, zwłaszcza że nie wymaga zmiany okablowania.

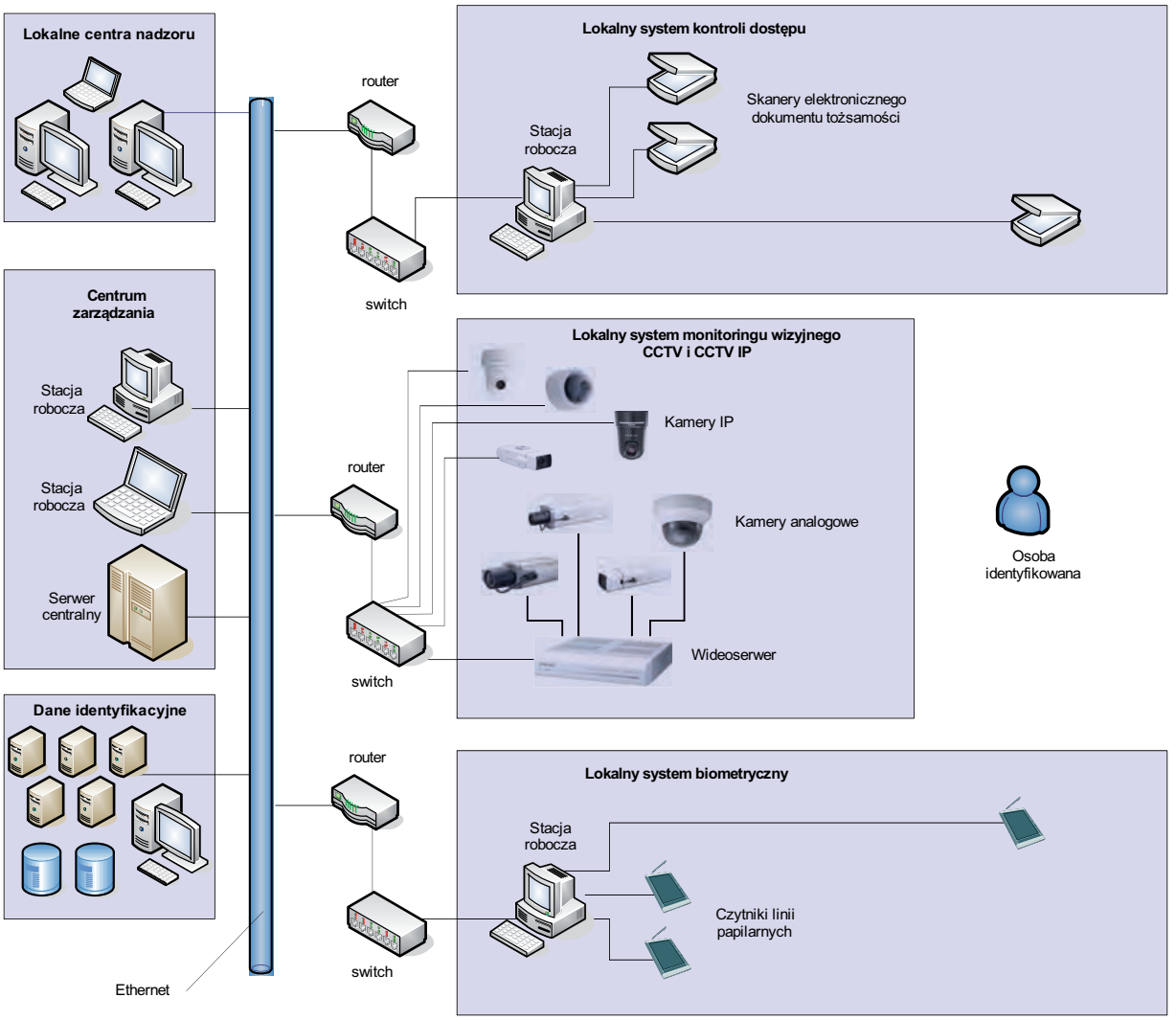
Gdy użytkownik weryfikuje się poprzez urządzenie biometryczne i weryfikacja jest pozytywna, wysyłany jest do systemu numer identyfikacyjny użytkownika, podobnie jak przy użyciu karty. Format jest zgodny ze stosowanym powszechnie w kartach. Decyzję o przyznaniu dostępu podejmuje urządzenie sterujące. Również kontrola drzwi i monitoring realizowane są przez system, a nie urządzenie biometryczne. Niektóre czytniki biometryczne mają wejście dla czytnika kart. Wówczas użytkownik korzysta ze swojej karty i nie musi wpisywać numeru ID na klawiaturze. Urządzenia z czytnikami biometrycznymi mogą współpracować z różnymi technologiami, jak np. karty ***smart cards,*** interfejs Wiegand, pasek magnetyczny, kod paskowy. Często stosuje się format 26-bitowy Wiegand oraz pasek magnetyczny ANSI. Karty zbliżeniowe mogą również być stosowane, gdyż na wyjściu mają format Wiegand. We wszystkich tego typu systemach zarządzanie wzorami biometrycznymi odbywa się w samych urządzeniach biometrycznych, a nie w panelu kontrolnym danego systemu. Jeżeli do systemu podłączonych jest wiele czytników biometrycznych, to może wystąpić problem związany z liczbą użytkowników. Niektóre urządzenia biometryczne pozwalają na rozwiązanie tego problemu w taki sposób, że wszystkie czytniki biometryczne zostają połączone w sieć zarządzającą wzorami.

4. Istota zintegrowanego rozproszonego systemu bezpieczeństwa

Stosowanie niezintegrowanych (skupionych) elektronicznych systemów bezpieczeństwa nie gwarantuje w pełnym zakresie przeciwdziałania zagrożeniom. Dlatego też konieczne staje się zintegrowanie ich przez tworzenie nadrzędnych centrów zarządzania, do których przesyłane byłyby informacje z poszczególnych systemów, a następnie analizowane w celu wykrycia zagrożenia (w szczególności identyfikacja osób i sprawdzenie, czy nie są podejrzane o działalność przestępczą).

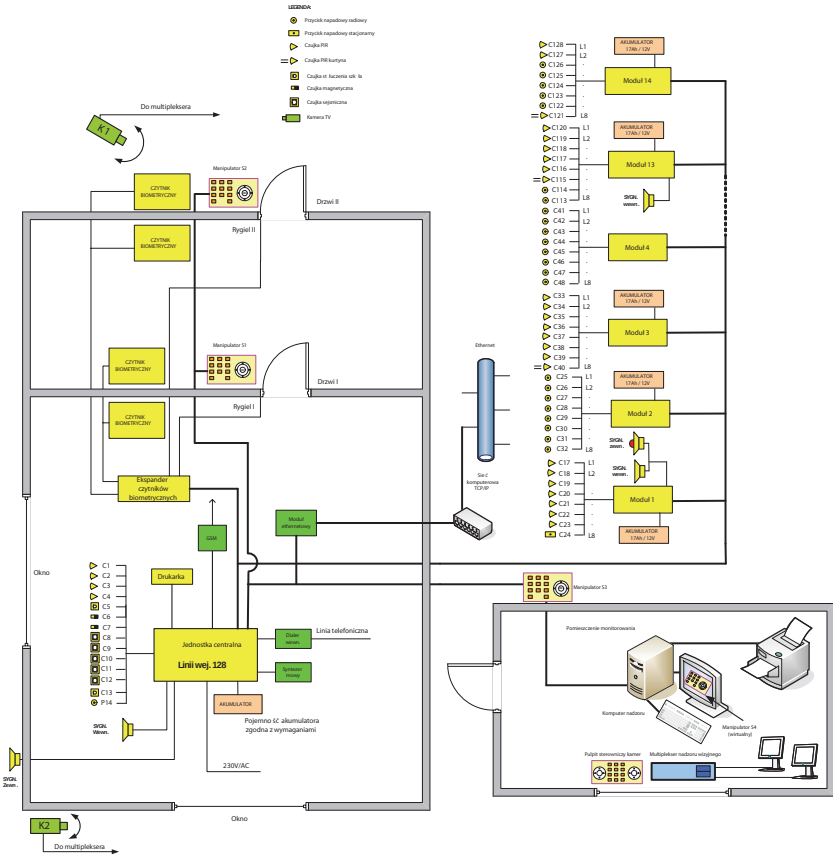
Zintegrowany system bezpieczeństwa (rys. 3) do identyfikacji osób wykorzystuje informacje z lokalnych systemów kontroli dostępu, monitoringu wizyjnego i biometrycznych, zainstalowanych w chronionym obiekcie (np. baza wojskowa, lotniska itp.) i połączonych siecią Ethernet z centrum zarządzania, lokalnymi centrami nadzoru i systemami bazodanowymi zawierającymi dane identyfikacyjne osób.

System monitoringu wizyjnego pełni podwójną rolę. Z jednej strony jest przeznaczony do obserwacji i rejestracji zdarzeń, które wystąpią w zasięgu kamer. Z drugiej strony obraz uzyskany z kamer znajdujących się przy wejściach do chro-



Rys. 3. Ogólny schemat zintegrowanego systemu bezpieczeństwa obiektu

Fig. 3. General scheme of integrated security system of object



Rys. 4. Schemat blokowy rozproszonego systemu bezpieczeństwa
Fig. 4. Block scheme of distracted security system

nionego budynku (lub też stref czy pomieszczeń specjalnych) jest przesyłany do centrum zarządzania. Dzięki zainstalowanemu oprogramowaniu analizującemu cechy biometryczne twarzy możliwe jest uwierzytelnienie osób poruszających się w obiekcie.

Centrum zarządzania jest jednostką nadrzędną w stosunku do lokalnych systemów. Zarządza ono całym zintegrowanym systemem bezpieczeństwa (np. dodanie nowych kamer IP, wideoserwerów, czytników biometrycznych wraz z ich konfiguracją) i jednocześnie archiwizuje informacje z poszczególnych urządzeń. Lokalne centra nadzoru pozwalają na tworzenie i podejmowanie decyzji w przypadku lokalnego zasięgu zdarzeń kryzysowych.

5. Syntetyczny opis rzeczywistego rozproszonego systemu bezpieczeństwa

Na rys. 4 przedstawiono zmodyfikowany rozproszony system bezpieczeństwa, znacznie rozbudowany i zmodernizowany poprzez wprowadzenie biometrycznych czytników linii papilarnych palca użytkownika upoważnionego. Znaczna modyfikacja, zrealizowana na przełomie lat 2008/2009, wynikała z potrzeb i wymagań obiektu specjalnego przeznaczenia. Wprowadzono jednostkę mikroprocesorową o 128 liniach wejściowych, dobudowano znaczną liczbę modułów rozszerzających (na dwóch magistralach jest ich czternaście). Znacznie rozbudowano pomieszczenie ochrony, w którym system bezpieczeństwa jest monitorowany. Tam też znajduje się komputer nadzorujący pracę systemu bezpieczeństwa (SSWiN i KD). Kontrola dostępu jest realizowana przez urządzenia z czytnikami biometrycznymi czytającymi linie papilarne użytkowników. W pomieszczeniu znajduje się również 16-wejściowy multiplekser cyfrowy z rejestracją zdarzeń na 4 dyskach HDD o pojemności po 700 GB każdy. Tam też znajdują się dwie drogi monitorowania: telekomunikacyjnego i radiowego. Elektroniczny system bezpieczeństwa został wyposażony w cztery manipulatory LCD, w tym jeden wirtualny. Dwa manipulatory LCD współpracują w systemie kontroli dostępu przy obsłudze pomieszczenia specjalnego przeznaczenia. Również to pomieszczenie zostało wyposażone w specjalne drzwi z atestowanymi zamkami mechanicznymi. Kontrola dostępu współpracuje również ze zworami elektromagnetycznymi (wynika to z logistyki obiektu). Z pomieszczenia monitorowania są sterowane szybkoobrotowe głowice kamer TV oraz ich obiektywy – zoomy z dobranymi ogniskowymi. Rezerwowe źródła zasilania (akumulatory) umożliwiają pracę systemu bezpieczeństwa przez co najmniej 72 h w przypadku awarii zasilania zasadniczego (230 V). Kamery monitoringu wizyjnego współpracują z oświetlaczami podczerwonymi wewnętrznymi o zasięgu od 8 m do 25 m oraz zewnętrznymi o zasięgu ok. 50 m.

Warto również wspomnieć o mechanicznych zabezpieczeniach zaproponowanych i zrealizowanych w obiekcie rzeczywistym specjalnego przeznaczenia. Są to specjalne okna z szybami kategorii odpowiedniej do tego typu pomieszczeń. W pomieszczeniach (rys. 4) zostały zainstalowane atestowane stalowe drzwi (I i II) z szeregiem zamków z atestami. Rygle elektromagnetyczne są sterowane biometrycznymi czytnikami linii papilarnych (z rejestracją wej/wyj). System kontroli dostępu zastosowany w pomieszczeniu (rys. 1), zrealizowany na bazie tej samej jednostki mikroprocesorowej (INTEGRA 128), chroni również wybrane pomieszczenie przeciwpożarowo. Jest zrealizowana zasada współpracy KD i systemu przeciwpożarowego (względy bezpieczeństwa). Pomieszczenia mają specjalną konstrukcję. Ściany, podłogi, sufity są chronione czujkami sejsmicznymi klasy S. Podobnymi czujkami są chronione sejfy pancerne. Warto wspomnieć o kompatybilności elektromagnetycznej, o zakłóceniach elektromagnetycznych, które stanowią bardzo ważny problem w systemach bezpieczeństwa o tak skomplikowanej budowie. Centrala alarmowa współpracuje z siecią informatyczną za pośrednictwem modułu ethernetowego. Taka metoda pozwala zdalnie zarządzać i administrować elektronicznym systemem bezpieczeństwa. System jest jednak wrażliwy na zakłócenia radioelektryczne, więc powinien być wykonany bardzo starannie. Ze względów bezpieczeństwa wszystkie pomieszczenia są wyposażone w metalowe siatki podtynkowe tworzące barierę elektromagnetyczną.

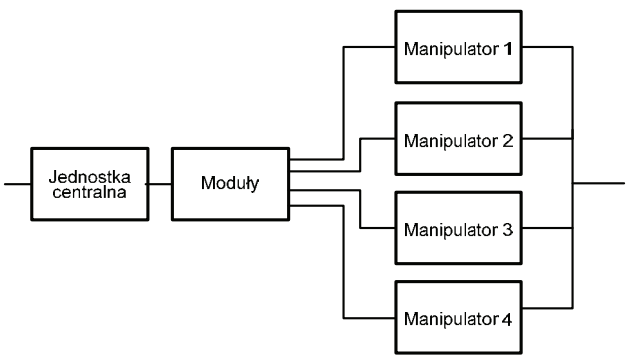
Wszystkie analizowane elektroniczne systemy bezpieczeństwa były nadzorowane wprost za pośrednictwem komputerów ze specjalnym oprogramowaniem, a systemom nadano adresy IP, co umożliwiło nadzór, zarządzanie i administrowanie za pośrednictwem sieci informatycznej.

Szczegółowa analiza układu blokowego (rys. 4) wraz z zebranymi danymi o charakterze niezawodnościowo-eksploatacyjnym (uszkodzenia sytemu, czasy postoju, napraw i ponownego przywrócenia do stanu zdatności) umożliwia zbudowanie modelu niezawodnościowo-eksploatacyjnego.

6. Model eksploatacyjno-niezawodnościowy rzeczywistego elektronicznego systemu bezpieczeństwa

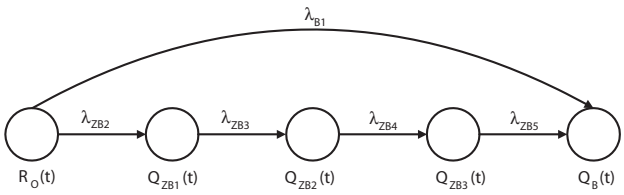
Model eksploatacyjno-niezawodnościowy (rys. 5) powstał w wyniku analizy rzeczywistego elektronicznego systemu bezpieczeństwa (rys. 4). Ze względu na duży stopień komplikacji rzeczywistego systemu bezpieczeństwa, zastosowano metodę niezbędnych uproszczeń, ale takich, które nie wypaczą logiki badań [8, 9]. Wszystkie czternaście moduły rozszerzające zawarte w elektronicznym systemie bezpieczeństwa zostały przedstawione w postaci jednego bloku i dołączone do bloku jednostki mikroprocesorowej (centralnej). Ze względów logistycznych do magistral zostały dołączone cztery manipulatory LCD, w tym jeden wirtualny. Tak zbudowany schemat eksploatacyjno-niezawodnościowy stanowi tzw. mieszany model niezawodnościowy. Można tu mówić o problemie nadmiarowości. Z punktu widzenia eksploatacji i niezawodności można wyróżnić nadmiarowość strukturalną, funkcjonalną, parametryczną, informacyjną, wytrzymałościową, czasową i elementową. Podane nadmiarowości nie są nigdy realizowane jednocześnie, nawet w trudnych i rozległych elektronicznych systemach bezpieczeństwa.

Analizując szczegółowo schemat z rys. 4 i jego uproszczony schemat niezawodnościowy (rys. 5) można stwierdzić, że mogą mieć miejsce wszystkie wymienione nadmiary. Jednak do badań szczególnie istotne są dwa nadmiary: strukturalny (przejście na rezerwowe źródło zasilania w przypadku awarii źródła zasadniczego) i funkcjonalny (kilka manipulatorów LCD, w tym wirtualny). Ten ostatni nadmiar funkcjonalny jest w tym przypadku bardzo ważny ze względu na logikę i procedury obowiązujące w tego typu obiektach specjalnego znaczenia.



Rys. 5. Schemat niezawodnościowy systemu bezpieczeństwa
Fig. 5. Structural flow reliability chart of the security system

W wyniku analizy blokowego schematu niezawodnościowego (uproszczonego) zaproponowano graf relacji zachodzących w rozproszonym systemie bezpieczeństwa (rys. 6).



Rys. 6. Relacje zachodzące w systemie bezpieczeństwa, gdzie: $R_O(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie pełnej zdatności, $Q_{ZB}(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa, $Q_B(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zawodności bezpieczeństwa, λ_{B1} – intensywność przejść central i modułów, λ_{ZB2}, λ_{ZB3}, λ_{ZB4}, λ_{ZB5} – intensywność przejść manipulatorów

Fig. 6. Relations in the security system, where: $R_O(t)$ – function of probability of system staying in the state of full ability, $Q_{ZB}(t)$ – function of probability of system staying in the state of the impendency over safety, $Q_B(t)$ – function of probability of system staying in the state of unreliability of safety, λ_{B1} – failure intensity of the control and indicating equipment and the modules, λ_{ZB2}, λ_{ZB3}, λ_{ZB4}, λ_{ZB5} – failure intensity of the manipulators

Jeżeli zastosuje się bardzo skomplikowane przekształcenia matematyczne, to można otrzymać zależności, które pozwolą wyznaczyć wartości prawdopodobieństw przebywania rozważanego (rzeczywistego) elektronicznego systemu bezpieczeństwa w odpowiednich stanach:

– stan pełnej zdatności R_0:

$$R_0(t) = e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t} \tag{1}$$

– stan zagrożenia bezpieczeństwa Q_{ZB1}:

$$Q_{ZB1}(t) = \lambda_{ZB2} \cdot \left[\frac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t} - e^{-\lambda_{ZB3}\cdot t}}{\lambda_{ZB3} - \lambda_{B1} - \lambda_{ZB2}} \right] \tag{2}$$

– stan zagrożenia bezpieczeństwa Q_{ZB2}:

$$Q_{ZB2}(t) = \lambda_{ZB2} \cdot \lambda_{ZB3} \cdot \left[\begin{array}{l} \dfrac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4}\right)\cdot\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3}\right)} - \\ - \dfrac{e^{-\lambda_{ZB3}\cdot t}}{\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3}\right)\cdot\left(\lambda_{ZB3}-\lambda_{ZB4}\right)} + \\ + \dfrac{e^{-\lambda_{ZB4}\cdot t}}{\left(\lambda_{ZB3}-\lambda_{ZB4}\right)\cdot\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4}\right)} \end{array} \right] \tag{3}$$

– stan zagrożenia bezpieczeństwa Q_{ZB3}:

$$Q_{ZB3}(t) = \lambda_{ZB2}\cdot\lambda_{ZB3}\cdot\lambda_{ZB4}\cdot \left[\begin{array}{l} \dfrac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{\left(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5}\right)\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4}\right)\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3}\right)} - \\ - \dfrac{e^{-\lambda_{ZB3}\cdot t}}{\left(\lambda_{ZB5}-\lambda_{ZB3}\right)\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3}\right)\left(\lambda_{ZB3}-\lambda_{ZB4}\right)} + \\ + \dfrac{e^{-\lambda_{ZB4}\cdot t}}{\left(\lambda_{ZB5}-\lambda_{ZB4}\right)\left(\lambda_{ZB4}-\lambda_{ZB3}\right)\left(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4}\right)} - \\ - \dfrac{e^{-\lambda_{ZB5}\cdot t}}{\left(\lambda_{ZB5}-\lambda_{ZB3}\right)\left(\lambda_{ZB5}-\lambda_{ZB4}\right)\left(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5}\right)} \end{array} \right] \tag{4}$$

– stan zawodności bezpieczeństwa Q_B:

$$Q_B(t)=\frac{\lambda_{B1}}{\lambda_{B1}+\lambda_{ZB2}}\cdot\left[1-e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}\right]+\lambda_{ZB2}\cdot\lambda_{ZB3}\cdot\lambda_{ZB4}\cdot\lambda_{ZB5}\cdot$$
$$\cdot\left[\frac{-e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{(\lambda_{B1}+\lambda_{ZB2})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})}+\right.$$
$$+\frac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot\lambda_{ZB3}\cdot(\lambda_{ZB3}-\lambda_{ZB4})\cdot(\lambda_{ZB5}-\lambda_{ZB3})}-$$
$$-\frac{e^{-\lambda_{ZB4}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{ZB3}-\lambda_{ZB4})\cdot\lambda_{ZB4}\cdot(\lambda_{ZB5}-\lambda_{ZB4})}+$$
$$+\frac{e^{-\lambda_{ZB5}\cdot t}}{\lambda_{ZB5}\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})\cdot(\lambda_{ZB5}-\lambda_{ZB4})\cdot(\lambda_{ZB5}-\lambda_{ZB3})}+$$
$$\left.+\frac{1}{(\lambda_{B1}+\lambda_{ZB2})\cdot\lambda_{ZB3}\cdot\lambda_{ZB4}\cdot\lambda_{ZB5}}\right] \quad (5)$$

Oznaczenia w powyższych zależnościach są następujące: t – czas, λ_{B1} – intensywność przejść central i modułów, λ_{ZB} – intensywność przejść manipulatora LCD

7. Obliczenia wskaźników niezawodnościowo-eksploatacyjnych

Do obliczeń przyjęto kilka istotnych danych dotyczących badanych systemów: czas obserwacji systemu: 1 rok = 8760 h, liczba badanych systemów: 10 (jak na rys. 4 lub podobnych).

Otrzymane wartości prawdopodobieństw przebywania systemu w różnych stanach:

– stan pełnej zdatności systemu R_0: 0,9504
– stan zagrożenia bezpieczeństwa Q_{ZB1}: 0,039195
– stan zagrożenia bezpieczeństwa Q_{ZB2}: 0,000601
– stan zagrożenia bezpieczeństwa Q_{ZB3}: 0,000004
– stan zawodności bezpieczeństwa Q_B: 0,009798

Powyższe wskaźniki zostały wyliczone na podstawie równań (1)–(5) z wykorzystaniem autorskiego programu komputerowego wspomagania Decyzji Niezawodnościowo-Eksploatacyjnych Elektronicznych Systemów Nadzoru.

8. Zakończenie i wnioski

Przedstawione wyniki obliczeń wymagają komentarzy. Gdyby przyjąć za ostateczny wynik $R_0 = 0{,}9504$, a więc stan pełnej zdatności elektronicznego systemu bezpieczeństwa, to wynik ten nie byłby satysfakcjonujący. Należy brać jednak pod uwagę, czego dotyczą wskaźniki: Q_{ZB1}, Q_{ZB2}, Q_{ZB3}? Wyliczone wartości dotyczą stanu zagrożenia bezpieczeństwa wynikającego z niezdatności kolejnych trzech manipulatorów LCD (w systemie bezpieczeństwa jest ich cztery) lub innych czytników informacji, np. biometrycznych. Aby mieć pełny obraz pełnej zdatności elektronicznego systemu bezpieczeństwa (rys. 4), należy przyjąć pewne założenia:

– wszystkie manipulatory LCD (3 szt.) realizują identyczne funkcje,
– podobnie i czwarty manipulator lecz wirtualny (jednak rozpatrywany rozdzielnie),
– urządzenia z czytnikami biometrycznymi realizują zbliżone funkcje.

Jeśli przyjąć takie założenia, to całkowity stan pełnej zdatności elektronicznego systemu bezpieczeństwa można wyrazić równaniem (6)

$$R_{0(całk)}=R_0+Q_{ZB1}+Q_{ZB2}+Q_{ZB3}=0{,}9504+0{,}039195+$$
$$+0{,}000601+0{,}000004=0{,}9902 \quad (6)$$

Można więc przedstawić warunek (7), wystarczający dla analizowanego elektronicznego systemu bezpieczeństwa obiektu specjalnego przeznaczenia:

$$0{,}9504 \le R_{0całk.} \le 0{,}9902 \quad (7)$$

Analizując nierówność (7) można odczytać, że warunek granicy prawostronnej spełnia tylko manipulator wirtualny, a lewostronnej wszystkie manipulatory. Można przyjąć, że w podanym przedziale system bezpieczeństwa znajduje się w pełnej zdatności. W trakcie analizy elektronicznego systemu bezpieczeństwa wyposażonego w urządzenia z czytnikami biometrycznymi nie były brane pod uwagę wszystkie procedury dotyczące obiektu specjalnego przeznaczenia. Jeśli wszystkie cztery manipulatory są w stanie zawodności bezpieczeństwa (jest to przypadek możliwy), analizowany system bezpieczeństwa nie nadaje się do dalszej eksploatacji. W stosunku do poprzedniej wersji zostały zamienione pastylki Dallas (2 szt.) na czytniki biometryczne (2 szt.), znacznie bezpieczniejsze w eksploatacji i praktycznie całkowicie eliminujące manipulacje niesolidnych użytkowników. Biometryczne systemy identyfikacji to systemy precyzyjnie identyfikujące użytkownika, którego uprawnienia (wcześniej zapisane) umożliwiają wstęp na teren obiektu chronionego jednym lub kilkoma systemami alarmowymi. Tego typu konstrukcje nie należą do tanich i trzeba je stosować tam, gdzie bezpieczeństwo tego wymaga. Mogą to być obiekty o strategicznym znaczeniu. Stąd urządzenia czytników biometrycznych stosowane w systemach ochrony obiektów mają różne konstrukcje i różny stopień komplikacji. Proponowany przez autorów układ czytników biometrycznych współpracuje z systemami kontroli dostępu znanej firmy ROGER typu RAKS 4. Autorzy przedstawili bardzo złożony zintegrowany system bezpieczeństwa wraz z centrum zarządzania współpracujący za pośrednictwem sieci Ethernet. Lokalne centra nadzoru (CCTV, CCTV IP, lokalny system biometryczny oraz lokalny system KD) pozwalają na tworzenie i podejmowanie decyzji w przypadku lokalnego zasięgu zdarzeń kryzysowych. Zaproponowany zintegrowany systemu bezpieczeństwa jest kontrolowany i nadzorowany przez Centrum Zarządzania. Dla uproszczenia i tak skomplikowanego schematu, autorzy nie przedstawili samych systemów elektronicznego nadzoru. Tego typu zintegrowany system powinien być stosowany w obiektach szczególnego znaczenia np. tam gdzie jest zagrożone bezpieczeństwo narodowe.

Bibliografia

1. Dunstone T., Yager N.: *Biometric System and Data Analysis*. Springer, 2009.
2. Dąbrowski T. Będkowski L. *Podstawy Eksploatacji cz. II Podstawy niezawodności eksploatacyjnej*, WAT, Warszawa 2006

3. Harwood E.: DIGITAL CCTV. A Security Professional's Guide. Butterworth Heinemann, 2007.
4. Hołyst B.: *Terroryzm*. Tom 1 i 2. Wydawnictwa Prawnicze LexisNexis, Warszawa 2009.
5. Instrukcje serwisowe systemów: DSC, RISCO, ROGER, SATEL, SONY.
6. Materiały Informacyjne Zakładu Elektroniki COMPAS, Jabłonna 2009.
7. Norma PN-EN 50132-7:2003: Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 7: Wytyczne stosowania.
8. Norman T.: *Integrated security systems design*. Butterworth Heinemann, 2007.
9. Szulc W. Rosiński A.: Prace własne dot. Elektronicznych Systemów Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie, Warszawa 2008–2010.
10. Szulc W., Rosiński A.: *Problemy eksploatacyjno-niezawodnościowe rozproszonego systemu bezpieczeństwa.* Zabezpieczenia Nr 1 (47)/2006, wyd. AAT, Warszawa 2006.
11. Tistarelli M., Li S. Z., Chellappa R.: *Handbook of Remote Biometrics for Surveillance and Security*. Springer-Verlag 2009.

Analysis of operating features and infallibility of safety systems under the computer surveillance

Abstract: In recent years a rapid development of biometric techniques has been observed. These techniques allow for the identification of persons based on some unique characteristic such as the size and shape of hands, fingerprints, eyes and voice. The development of electronic systems and microprocessors together with the simultaneous price reduction have made feasible the application of biometric sensors in many electronic safety systems. In this article it is presented the concept of some integrated electronic safety systems used for selected objects under the computer surveillance. In these systems the biometric methods for the identification of persons has been applied. In particular, territorially extended objects have been considered. The authors for many years have been involved in investigating the operating features and infallibility of electronic safety systems building models which give the necessary parameters.

Keywords: safety system, reliability, biometrics

doc. dr inż. Waldemar Szulc

Od 1965 roku pracownik naukowy Politechniki Warszawskiej na Wydziałach: Komunikacji, Elektroniki, Instytutu Transportu oraz na Wydziale Transportu. Zajmował się problematyką: Telekomunikacji, Radiokomunikacji, Radiolokacji, Podstaw Elektroniki i Elektroniki ze szczególnym uwzględnieniem układów dla potrzeb Transportu oraz Elektronicznymi Systemami Bezpieczeństwa Obiektów. Jest autorem lub współautorem ponad 10 patentów oraz autorem lub współautorem ponad 52 wdrożeń urządzeń elektronicznych dla potrzeb PKP. Jest autorem lub współautorem ponad 150 publikacji. Brał udział w ponad 35 pracach o charakterze naukowo-badawczym. Obecnie jest Prodziekanem Wydziału Informatyki Stosowanej i Technik Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie. Jest autorem lub współautorem wielu unikalnych rozwiązań z dziedziny Bezpieczeństwa Obiektów o charakterze specjalnym. Współautor koncepcji, zaprojektowania i uruchomienia „Zespołu Laboratorium Systemów Bezpieczeństwa" w Wyższej Szkole Menedżerskiej w Warszawie.

e-mail: waldemar.szulc@mac.edu.pl

dr inż. Adam Rosiński

Adiunkt w Zakładzie Telekomunikacji w Transporcie na Wydziale Transportu Politechniki Warszawskiej. Zainteresowania naukowe obejmują elektronikę (analogową i cyfrową) oraz zagadnienia związane z niezawodnością, eksploatacją, diagnostyką i projektowaniem elektronicznych systemów bezpieczeństwa (Systemy Sygnalizacji Włamania i Napadu, Systemy Monitoringu Wizyjnego, Systemy Kontroli Dostępu, Systemy Sygnalizacji Pożarowej, Dźwiękowe Systemy Ostrzegawcze, monitoring systemów, integracja systemów). Jest czynnym uczestnikiem wielu krajowych i międzynarodowych konferencjach naukowych. Ma w dorobku naukowym (jako autor lub współautor) ponad 60 publikacji, a także wielu unikalnych rozwiązań z dziedziny bezpieczeństwa obiektów o charakterze specjalnym.

e-mail: adro@it.pw.edu.pl