CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(88)/2012

ZABEZPIECZENIA

WWW.ZABEZPIECZENIA.COM.PL • E-MAIL: ZABEZ@ZABEZPIECZENIA.COM.PL

W NUMERZE:

Większa rentowność dzięki dyskretnemu i przystępnemu cenowo rozwiązaniu do nadzoru z funkcjami PTZ? **To proste.**

Czy chcą Państwo poprawić bezpieczeństwo w swoim sklepie? A może także zwiększyć efektywność operacyjną i rentowność? Oba te cele pomoże zrealizować rozwiązanie nadzoru wizyjnego.

Kamery Axis z linii M z funkcjami obrót/pochylenie/zbliżenie udostępniają materiał wizyjny jakości HDTV, alarmy w czasie rzeczywistym oraz inne inteligentne i przydatne możliwości. Dzięki nim można między innymi zwalczać kradzieże w sklepach, zapobiegać brakowi towaru na półkach oraz monitorować kolejki do kas.

Ze względu na elastyczne funkcje obrót/pochylenie/zbliżenie, niewielkie rozmiary i prostą instalację kamery AXIS z serii M50 umożliwiają łatwą i dyskretną obserwację wszystkiego, co dzieje się w sklepie.

Niewielka kamera. Wielkie możliwości. Łatwy wybór.

Przyjmij punkt widzenia Axis. Bądź zawsze o krok do przodu.
Odwiedź www.axis.com/ptz

Kopułkowa kamera sieciowa PTZ AXIS z serii M50 • Jakość materiału wizyjnego do poziomu HDTV 720p • Funkcje obrotu, pochylenia i zbliżenia oraz ultradyskretna konstrukcja • Zasilanie przez sieć Ethernet • Wbudowany mikrofon • Ochrona klasy IP51 • Gniazdo kart pamięci MicroSD/SDHC

AXIS COMMUNICATIONS

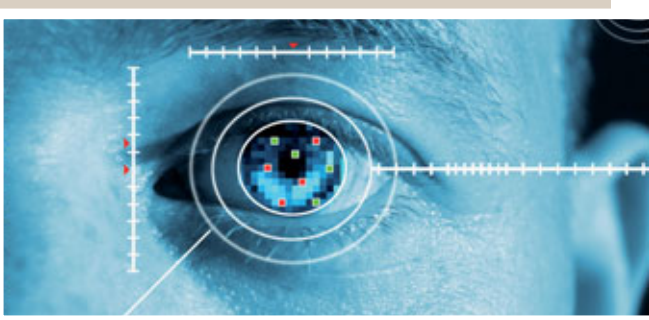
Spis treści

CZASOPISMO ZABEZPIECZENIA 6/2012

Axis wprowadza do swojej oferty miniaturowe kamery HDTV przeznaczone do systemów dyskretnego dozoru wizyjnego **30**

Systemy klucza generalnego – Assa Abloy **38**

Stosowanie środków bezpieczeństwa fizycznego w ochronie informacji niejawnych **46**



Biometria w kontekście problemów prawnych **68**

Samsung wprowadza kompaktową, płaską 1,3-megapikselową sieciową kamerę kopułkową LiteNet

Samsung powiększył serię sieciowych kamer HD o 1,3-megapikselową płaską kamerę kopułkową. Model **SND-5010** o wymiarach zaledwie 100x115x42 mm jest niedrogim urządzeniem do nadzoru wizyjnego HD, które można zastosować w miejscach o ograniczonej przestrzeni, takich jak windy, przedsionki, klatki schodowe, niewielkie sklepy lub wnętrza środków transportu.

Zgodny ze standardami ONVIF model SND-5010 umożliwia kompresję obrazów metodą H.264 oraz MJPEG. Pozwala też na równoczesną transmisję obrazów różniących się jakością i poklatkowością do wielu lokalizacji i może współpracować z monitorem HD o proporcjach 16:9 (1280×720). Dzięki temu możliwa jest jednoczesna realizacja kilku funkcji, takich jak lokalny monitoring chronionego obszaru prowadzony w czasie rzeczywistym, rejestracja obrazów ze wszystkich kamer i przeglądanie obrazów na ekranach urządzeń przenośnych, takich jak smartfony, za pomocą aplikacji Samsung iPOLiS.

Kamera SND-5010, którą wyposażono w stałoogniskowy obiektyw 3 mm, ma funkcję wykrywania zmian pola widzenia, która spowoduje wywołanie alarmu, gdy obiektyw zostanie zamalowany farbą lub w przypadku innej nieautoryzowanej zmiany standardowego pola widzenia kamery.

Pomimo kompaktowych rozmiarów urządzenia SND-5010 wyposażono w wiele funkcji ułatwiających pracę instalatorom, do których należą: cztery programowalne strefy detekcji ruchu, dwanaście programowalnych stref prywatności oraz możliwość zasilania metodą PoE. Kamera ta może pracować w trybie dzień/noc i wykorzystuje technologię *Samsung Super Noise Reduction* (SSNR) trzeciej generacji w celu eliminacji szumów obrazu powstałych wskutek niedostatecznego oświetlenia, dzięki czemu umożliwia oszczędne wykorzystanie pasma sieciowego lub przestrzeni dyskowej.

W pełni kompatybilna z bezlicencyjnym oprogramowaniem Samsung NET-i Viewer kamera SND-5010 może być konfigurowana za pośrednictwem wielojęzycznej strony internetowej, która ułatwia wprowadzenie wymaganych ustawień.

Pozostałe modele kamer z linii Samsung LiteNet to:

– SNB-5001 – kamera sieciowa o rozdzielczości 1,3 Mpx,
– SND-5011 – sieciowa kamera kopułkowa o rozdzielczości 1,3 Mpx, ze stałoogniskowym obiektywem 3 mm,
– SND-5061 – sieciowa kamera kopułkowa o rozdzielczości 1,3 Mpx, ze zmiennoogniskowym obiektywem 3~8 mm,
– SNB-7001 – sieciowa kamera Full HD o rozdzielczości 3 Mpx,
– SND-7011 – sieciowa kamera Full HD o rozdzielczości 3 Mpx, ze stałoogniskowym obiektywem 3 mm,
– SND-7061 – sieciowa kamera kopułkowa Full HD o rozdzielczości 3 Mpx, ze zmiennoogniskowym obiektywem 3~8 mm.

Bezpośr. inf. David Solomons
DRS Marketing

Nowe rejestratory CCTV współpracujące z systemem kontroli dostępu ROGER

Udostępnione przez firmę **ROGER** oprogramowanie PR Master w wersji 4.5 umożliwia integrację systemu kontroli dostępu z rejestratorami wizyjnymi pracującymi w systemach CCTV. Dzięki temu są większe możliwości integracji systemu kontroli dostępu **RACS 4**. Aktualnie oprócz współpracy z systemami rejestracji czasu pracy i systemami SSWiN możliwa jest również integracja z systemami telewizji dozorowej dzięki kolejnym modelom rejestratorów DVR. Dotychczas możliwe było połączenie systemu ROGER z rejestratorem stacjonarnym BCS0804LE-A firmy Dahua oraz kartą przechwytującą GV600/4 firmy Geovision. Obecnie do tej listy dodano rejestratory stacjonarne DS-7204HVI-ST firmy HIK Vision oraz Raiden HDR-7204. Integracja polega na powiązaniu zdarzeń w systemie kontroli dostępu z zarejestrowanym obrazem pochodzącym z kamer CCTV.

Po skonfigurowaniu połączenia systemu RACS 4 z rejestratorem oprogramowanie PR Master umożliwia odtwarzanie fragmentów zarejestrowanego materiału wizyjnego związanych z wybranymi zdarzeniami zaistniałymi na kontrolowanych przejściach, a także podgląd obrazu z kamer podłączonych do rejestratora w czasie rzeczywistym.

Wdrożone rozwiązanie znajduje zastosowanie wszędzie tam, gdzie istnieje potrzeba wyświetlenia materiału wizyjnego pokazującego zdarzenia w systemie kontroli dostępu bez konieczności ręcznego przeszukiwania wszystkich nagrań zapisanych w rejestratorze. W ramach integracji program PR Master nie musi być stale uruchomiony.

Bezpośr. inf. Kamil Stadnicki
ROGER

IVA – przyszłość CCTV

Stosowanie rozbudowanych systemów telewizji dozorowej rozpowszechnia się coraz bardziej. W większości dużych obiektów budowlanych są dziesiątki kamer i tylko jeden operator do ich nadzoru, co nie jest najlepszym rozwiązaniem, ponieważ jedna osoba nie jest w stanie efektywnie przeglądać obrazów z wielu kamer, np. 64, i prawidłowo reagować na każdą sytuację wymagająca interwencji. W takich przypadkach pomocna jest innowacyjna technologia, na przykład w postaci oprogramowania **IVA** (*Intelligent Video Analytic Software*) amerykańskiej firmy Aventura.

Łatwa i intuicyjna konfiguracja programu czyni z niego idealne narzędzie wspomagające.

Umożliwia on między innymi:

– tworzenie wirtualnego ogrodzenia, którego przekroczenie wywołuje alarm lub powoduje inną akcję,
– zliczanie osób wchodzących, wychodzących przez jakieś przejście lub przebywających w danej strefie,
– wykrywanie przedmiotów pozostawionych w obserwowanej strefie lub zabranych z tej strefy,
– kontrolę ruchu pojazdów, np. wykrywanie samochodów zbyt długo parkujących w strefie, w której możliwy czas postoju jest ograniczony, lub wykrywanie samochodów zatrzymujących się na terenie, na którym obowiązuje zakaz zatrzymywania się,
– wykrywanie prób zasłonięcia kamery,
– eliminację fałszywych alarmów, np. wywoływanych przez liście falujące na wietrze.

Narzędzie to diametralnie polepsza warunki pracy operatora systemu monitoringu wizyjnego, ponieważ nie musi on koncentrować całej swej uwagi na wypatrywaniu szczegółów obserwowanych scen. Obrazy różnych wyznaczonych stref mogą być analizowane indywidualnie. W ten sposób operator jest informowany o zaistnieniu konkretnych, potencjalnie niebezpiecznych sytuacji. W razie wykrycia niedozwolonej czynności system reaguje alarmem, komunikatem lub wykonaniem innej zaprogramowanej czynności.

Więcej informacji na temat *Intelligent Video Analysis* można uzyskać u wyłącznego polskiego dystrybutora, którym jest firma **ZBAR** z Łodzi (*www.zbar.com.pl*).

Bezpośr. inf. Krystian Witczak, Karolina Zasada
ZBAR

VX INFINITY

nowa seria czujek OPTEX

Czujki zewnętrzne VX-402 są dostępne na rynku od kilkunastu lat. W tym czasie zostały zamontowane w tysiącach obiektów w Polsce, a zastosowane w nich rozwiązania technologiczne znalazły wielu naśladowców.

Po zaprezentowaniu serii nowych czujek wewnętrznych **RX CORE** (kolejny model – czujka dualna **RXC-DT** – będzie dostępny na początku 2013 r.) **OPTEX** zapowiada wprowadzenie do sprzedaży czujek, które zastąpią klasyczny model VX-402. Pierwsze informacje na temat **VX INFINITY** mówią o sześciu modelach w różnych konfiguracjach.

Podstawowa zmiana to wprowadzenie cyfrowego algorytmu detekcji SMDA (*Super Multi Dimension Analysis*), dzięki któremu uzyskano znacznie większą odporność czujki na zakłócenia pochodzące ze środowiska zewnętrznego, m. in. na światło słoneczne, wzrost i ruchy roślin, obecność zwierząt. Odporność ta jest 24-krotnie większa w porównaniu z poprzednim modelem. Drugą ważną innowacją jest zastosowanie antymaskingu z cyfrową obróbką sygnału, która umożliwia przystosowanie się czujki do stopnia zabrudzenia soczewki. Pojawi się również model dualny (detektor PIR plus czujka mikrofalowa), przeznaczony do zastosowań specjalnych.

W celu dopasowania obszaru detekcji do prostokątnych przestrzeni, np. w przypadku umieszczenia czujki w niewielkiej odległości od płotu ograniczającego posesję, stosowane będą naklejki maskujące umieszczane na soczewce. Zwiększono liczbę pól detekcji i precyzję ich rozmieszczenia, co wpływa na spadek liczby fałszywych alarmów. Nowością jest także mniejsza obudowa wykonana ze znacznie bardziej odpornego na odbarwianie tworzywa ASA.

Serię VX INFINITY uzupełniają modele zasilane bateryjnie, przeznaczone do zastosowania w instalacjach bezprzewodowych.

Czujki będą dostępne u dystrybutorów OPTEX w pierwszym kwartale 2013 r. Ceny poszczególnych modeli nie są jeszcze znane.

Bezpośr. inf. Jacek Wójcik
OPTEX Security

FLIR LS

kompaktowe, przenośne kamery termowizyjne

LS to najnowsza seria kamer przenośnych marki **FLIR** umożliwiająca obserwację w całkowitej ciemności. Zakres jej zastosowań jest bardzo szeroki. Przykładowo – kamera **FLIR LS64** generuje obraz termowizyjny o rozdzielczości 640×480 pikseli. Użytkownicy, którzy nie potrzebują tak dobrego obrazu, mogą wybrać model **LS32** o rozdzielczości 320×240 pikseli. Wszystkie kamery są wyposażone

w wewnętrzne oprogramowanie zapewniające tworzenie wyraźnego i ostrego obrazu termicznego bez potrzeby ręcznej regulacji parametrów kamery. Ponadto każda kamera termowizyjna z serii LS ma funkcję InstAlert. Umożliwia ona oznaczenie najcieplejszego obiektu kolorem czerwonym. Właściwość ta ułatwia szybkie wykrycie podejrzanych obiektów widocznych na obrazie termowizyjnym.

Bezpośr. inf. Jakub Sobek
Linc Polska

Axon Power Video Protector Twist

W odpowiedzi na sugestie instalatorów inżynierowie z krakowskiej firmy **HSK DATA** wprowadzają na rynek nowe urządzenie **AXON Power Video Protector Twist**.

Urządzenie to jest przeznaczone do ochrony przeciwprzepięciowej kamer i rejestratorów w analogowych systemach CCTV wykorzystujących skrętkę komputerową do przesyłu sygnału wizyjnego i zasilania.

AXON Power Video Protector Twist zawiera dwa tory ochronne. Jeden służy do ochrony linii służącej do transmisji sygnału wizji, a drugi zabezpiecza obwód zasilania kamery.

W obu torach zastosowano rozbudowany system ochrony. Gazowe elementy ochronne odprowadzają większą część ładunku udarowego do ziemi, natomiast szybkie elementy półprzewodnikowe ograniczają przepięcia mogące pojawić się pomiędzy przewodami.

AXON Power Video Protector Twist z powodzeniem zastępuje dwa inne ochronniki, do tej pory stosowane osobno do ochrony linii zasilającej i transmisyjnej. Dzięki temu możliwe jest ograniczenie kosztów ochrony przeciwprzepięciowej analogowych systemów monitoringu wizyjnego. Urządzenie jest zgodne z wymaganiami normy EN-PN 61643-21.

Wojciech Zieliński
HSK DATA

Axon Video Protector 4

HSK DATA z Krakowa wprowadza na rynek kolejne wielokanałowe urządzenie z rodziny Axon Video Protector. Nowy ochronnik o nazwie **Axon Video Protector 4** jest przeznaczony do ochrony urządzeń elektronicznych pracujących w systemach analogowej telewizji dozorowej, takich jak kamery, monitory i rejestratory sygnału wizyjnego.

Axon Video Protector 4 zawiera cztery niezależne tory, z których każdy wyposażony jest w elementy ochronne ograniczające przepięcia pojawiające się pomiędzy linią transmisyjną a przewodem PE. W urządzeniu zastosowano również elementy ograniczające napięcie mogące wystąpić między linią sygnałową a ekranem kabla. Takie rozwiązanie umożliwia kompleksowe zabezpieczenie urządzeń podłączonych do ochronnika.

Axon Video Protector 4 doskonale sprawdzi się w popularnych małych systemach monitoringu wizyjnego wykorzystujących gotowe zestawy urządzeń zawierające cztery kamery.

Axon Video Protector 4 jest tańszy niż cztery pojedyncze ochronniki, dzięki czemu można zmniejszyć koszty ochrony przeciwprzepięciowej analogowych systemów monitoringu wizyjnego. Urządzenie spełnia wymagania normy EN-PN 61643-21.

Wojciech Zieliński
HSK DATA

Funkcja śledzenia obiektu w kamerze PTZ AutoDome HD serii 800

Bosch Security Systems wprowadza nową wersję oprogramowania (firmware 5.52) dla kamer **PTZ AutoDome HD serii 800**. Obejmuje ono nową funkcję *Intelligent Tracking* dla dwumegapikselowych kamer PTZ.

Funkcja *Intelligent Tracking* wykorzystuje oprogramowanie służące do inteligentnej analizy obrazu (IVA – *Intelligent Video Analysis*), wbudowane w kamery AutoDome, które w sposób ciągły analizuje obserwowane sceny, wykrywa i automatycznie śledzi obiekty poruszające się w polu widzenia kamery.

Użytkownicy mogą wykorzystywać oprogramowanie IVA firmy Bosch do określania warunków, w których aktywowana jest funkcja ciągłego śledzenia. Mogą na przykład zaprogramować kamerę w taki sposób, by śledziła wszystkie pojazdy poruszające się na określonym obszarze i w konkretnym kierunku.

Śledzenie obiektu można rozpocząć w dowolnym momencie, wskazując kliknięciem poruszający się cel widoczny na ekranie. Kamera skoncentruje się wtedy na jego śledzeniu i – w zależności od potrzeb – będzie wykorzystywać funkcje obrotu, pochylenia lub powiększenia. Kamera automatycznie przerwie śledzenie, gdy cel tymczasowo znajdzie się na obszarze maskowanej strefy prywatności lub ukryje się za innym obiektem. Zacznie go śledzić ponownie, gdy znowu pojawi się w jej polu widzenia.

Wysoka rozdzielczość kamery (HD 2 Mpx/1080p) oraz użycie obiektywu zmiennoogniskowego 20× w połączeniu z funkcją *Intelligent Tracking* praktycznie wyklucza możliwość przeoczenia podejrzanych wydarzeń i pozwala na dokładną rejestrację ważnych cech obserwowanych obiektów, które umożliwiają ich identyfikację. Szczegóły obrazu, takie jak rysy twarzy obserwowanych osób czy numery tablic rejestracyjnych pojazdów, zostaną dokładnie zarejestrowane nawet przy znacznej odległości od obserwowanych obiektów. Dzięki temu kamery PTZ AutoDome HD serii 800 z funkcją *Intelligent Tracking* oraz zautomatyzowaną funkcją monitorowania znakomicie sprawdzają się w systemach dozoru wizyjnego.

Funkcja *Intelligent Tracking* jest dostępna w kamerach AutoDome HD serii 800 oraz w kamerach sieciowych AutoDome serii 700. Daje to klientom możliwość zbudowania systemu monitoringu, który zapewnia obraz o rozdzielczości standardowej lub megapikselowej (HD).

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

C&C Partners Telecom
nowa siedziba na Śląsku

Oddział Handlowy **C&C Partners Telecom w Katowicach** ma nową siedzibę – **przy ulicy Malinowej 8**. 12 września 2012 roku odbyło się jej uroczyste otwarcie. Budynek, w którym mieści się katowickie biuro, jest nowoczesny, zbudowany z cegły, stali i szkła, otoczony zielenią. Charakter budowli doskonale oddaje charakter spółki. Cegła i stal dają poczucie stabilności i solidności, a szklane ściany dają szerokie horyzonty i dobrą perspektywę. Spółka C&C Partners Telecom działa na rynku od dwudziestu lat. Oferuje nowoczesne rozwiązania o najlepszej jakości oraz fachową pomoc specjalistów.

Uroczystość odbyła się w ogrodzie. Panował miły nastrój sprzyjający rozmowom. W tle słychać było dźwięki muzyki jazzowej w wykonaniu zespołu Srebro Quartet, utworzonego przez studentów Akademii Muzycznej w Katowicach. W tych okolicznościach firma C&C Partners Telecom podpisała umowę z Samsung Techwin Europe i tym samym kontynuuje dystrybucję produktów firmy Samsung.

Atrakcją była degustacja serów holenderskich, która podkreślała silny związek firmy C&C Partners Telecom z tym krajem.

C&C Partners Telecom założyli w 1992 dwaj spokrewnieni ze sobą Holendrzy, którzy działalność rozpoczęli od sprzedaży central telefonicznych na rozwijającym się polskim rynku telekomunikacyjnym. Od samego początku spółka dynamicznie się rozwijała, poszerzając swoją ofertę i dostosowując ją do potrzeb rynku. W 1998 roku dwaj pierwsi właściciele sprzedali ją międzynarodowemu holdingowi THK z siedzibą w Holandii, który wówczas zajmował się wyłącznie nowoczesnymi technologiami z zakresu telekomunikacji. Obecnie C&C Partners Telecom jest jedną z 70 spółek należących do Grupy TKH, a w jej ofercie, obok rozwiązań telekomunikacyjnych, znajdują się rozwiązania z zakresu teleinformatyki i zabezpieczeń.

Choć działalność C&C Partners Telecom od początku obejmowała obszar całego kraju, Holendrzy zdecydowali się na założenie centrali w Lesznie. Katowicki oddział handlowy został otwarty jako drugi, po warszawskim. Dynamicznie rozwijający się region południa Polski dawał i daje dobre perspektywy rozwoju firmy. Dlatego w 2000 roku zarząd spółki, chcąc być bliżej swoich obecnych i przyszłych partnerów, podjął decyzję o otwarciu oddziału w Katowicach.

Obecnie jest w nim zatrudnionych ośmiu pracowników. Ich miejsce pracy to przestronne pomieszczenia, częściowo przedzielone ścianami działowymi, częściowo przeszklone. Otwarta powierzchnia sprzyja współpracy zespołu, podczas gdy wspomniany podział daje każdemu pracownikowi wygodną przestrzeń do pracy. Poza gabinetem dyrektora, salą do telekonferencji oraz pomieszczeniami socjalnymi w biurze mieści się sala seminaryjna. Na szkolenia odbywające się na Malinowej 8 zespół C&C Partners Telecom zaprasza już dziś.

Bezpośr. inf. Iga Niemczyk
C&C Partners Telecom

Urządzenia Bosch spełniają wymagania normy kompatybilności elektromagnetycznej

Od lata 2014 roku wszystkie urządzenia antywłamaniowe oferowane na rynku wspólnotowym będą musiały być zgodne z wymaganiami nowej wersji normy europejskiej **EN 50130-4**. Czujki firmy **Bosch Security Systems** już teraz spełniają te wymogi.

EN 50130-4 to norma kompatybilności elektromagnetycznej (*electromagnetic compatibility* – EMC), która dotyczy systemów alarmowych stosowanych w budynkach i na zewnątrz, w środowiskach komercyjnych, przemysłowych i mieszkaniowych. Jej celem jest zapewnienie ich prawidłowego działania w przypadku wystąpienia zakłóceń elektromagnetycznych (*electromagnetic interference* – EMI).

W najnowszej wersji normy rozszerzony został zakres częstotliwości pola elektromagnetycznego, na które musi być odporne urządzenie wykorzystywane w systemach alarmowych. Poprzednia wersja wymagała odporności w zakresie częstotliwości od 80 MHz do 2,0 GHz. Najnowsza wersja normy rozszerza ten zakres aż do 2,7 GHz.

– *Zwiększenie wymagań normy jest związane ze wzrostem zakłóceń elektromagnetycznych w budynkach. Wynikają one z coraz większej popularności urządzeń wykorzystujących nowe, wyższe pasmo częstotliwości, takich jak telefony komórkowe i urządzenia z Wi-Fi. Zwiększając odporność czujek ruchu na zakłócenia elektromagnetyczne wywoływane przez systemy bezprzewodowe, Bosch Security Systems zwiększa skuteczność instalacji. Wykorzystywane w instalacjach urządzenia są również odporne na fałszywe alarmy* – podkreśla **Bożena Wicha**, Product Manager w Bosch Security Systems.

Chociaż producenci będą mieć obowiązek spełnienia zaostrzonych wymagań normy dopiero od lata 2014 roku, Bosch Security Systems już teraz dostosował do nich swoje czujki ruchu Blue Line Gen 2, czujki alarmowe ruchu Professional Series, czujki sufitowe DS938Z, DS9360, DS939 oraz czujkę zewnętrzną OD850.

Czujki ruchu Blue Line Gen 2 umożliwiają pokrycie powierzchni o wymiarach 12 x12 metrów od ściany do ściany, bez żadnych luk. Dzięki przetwarzaniu FSP (*First Step Processing*) są w stanie odróżnić ludzi od innych obiektów żywych, np. zwierząt domowych. Czujki alarmowe ruchu Professional Series są wyposażone w technologię SDF (*Sensor Data Fusion*), która umożliwia przetwarzanie sygnałów z maksymalnie pięciu różnych czujników przed podjęciem decyzji o sygnalizacji alarmu. Wpływa to na zwiększenie ich efektywności w porównaniu z tradycyjnymi czujkami ruchu. Czujki te znajdują zastosowanie w wielu miejscach, takich jak magazyny, sklepy, budynki rządowe i duże biura.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

SATEL wspiera działania GOPR

W tym roku **Górskie Ochotnicze Pogotowie Ratunkowe** obchodzi 60-lecie swojej działalności. Z okazji tego jubileuszu w dniach 7–9 września w miejscowości Karłów (w Górach Stołowych) odbyły się **XVIII zawody ratowników**. Firma **SATEL** po raz pierwszy miała przyjemność sponsorować tę imprezę.

Zawody polegały na pokonaniu przez trzyosobowy zespół ratowników trasy biegu terenowego o długości około dziewięciu kilometrów, na której umieszczono elementy techniczne alpinistyczne i taternickie stosowane w ratownictwie górskim. Konkurencje techniczne zorganizowano na Szczelińcu Wielkim. Udział wzięły drużyny trzyosobowe, a uczestników podzielono według kategorii wiekowej. Tegoroczne zadania, jakie wyznaczono drużynom, wymagały niezwykłej sprawności i dużego doświadczenia. Zdobycie miejsc na podium świadczyło o bardzo dobrym przygotowaniu, zaangażowaniu i determinacji.

Już od pięciu lat firma SATEL wspiera działania GOPR. Dbanie o bezpieczeństwo, życie i mienie ludzkie to dla firmy SATEL główny wyznacznik działalności. GOPR udziela w górach pomocy ludziom, których zdrowie lub życie jest zagrożone, zapobiega wypadkom oraz chroni środowisko górskie, dlatego wsparcie tej organizacji jest zgodne z głównym celem działalności firmy SATEL, jakim jest dbanie o bezpieczeństwo, życie i mienie ludzkie.

Bezpośr. inf. Agnieszka Pitrus
SATEL

Nowe kompaktowe kamery Bosch z serii Advantage Line

Bosch Security Systems rozszerza serię produktów **Advantage Line**. Wprowadza do niej trzy kompaktowe kamery analogowe.

Modele **VDC-275-10** i **VDN-276-10** są kamerami kopułkowymi przeznaczonymi do zastosowań wewnętrznych. Gwarantują wysoką rozdzielczość obrazu, również w złych warunkach oświetleniowych. Wyposażone są w przetwornik obrazu CCD 1/3" 960H, wykorzystują cyfrowy system tłumienia szumów i mają szeroki zakres dynamiki.

Nowa kamera kopułkowa **VDN-295-10**, przeznaczona do zastosowań wewnętrznych, zapewnia szeroki zakres dynamiki (funkcja Wide Dynamic Range) i jest wyposażona w zaawansowany system cyfrowego tłumienia szumów (3DNR). Umożliwia zaprogramowanie aż piętnastu stref prywatności.

Kamery są dostępne w wersji kolorowej (VDC) oraz w wersji dzień/noc (VDN). Modele VDN zapewniają wysoką jakość obrazu niezależnie od pory dnia. W zależności od natężenia oświetlenia kamera automatycznie zmienia tryb pracy z kolorowego na monochromatyczny.

Wszystkie trzy modele są łatwe w instalacji. Ustawienie obiektywu można regulować w trzech osiach. Rozmieszczenie czterech stref prywatności oraz opcje wykrywania ruchu można zaprogramować za pomocą prostego menu.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Bosch dba o bezpieczeństwo na polskich drogach

Kamery Bosch Security Systems są wykorzystywane w inteligentnych systemach bezpieczeństwa ruchu drogowego

Niedostosowanie prędkości pojazdów do warunków drogowych jest jedną z głównych przyczyn wypadków w Polsce. Do podwyższenia poziomu bezpieczeństwa na naszych drogach nie wystarczą zwykłe fotoradary. Potrzebne są inteligentne systemy, które, zamiast skupiać się na jednym czynniku, na przykład na nadmiernej prędkości, analizują szereg potencjalnych zagrożeń i mogą być wykorzystywane do kompleksowego monitorowania.

Od ponad sześciu lat spółka Bosch Security Systems współpracuje z firmą Neurosoft, która tworzy systemy służące do poprawy bezpieczeństwa ruchu drogowego. System Neurocar służy do wizyjnej detekcji i identyfikacji obiektów, którą umożliwiają kamery Bosch. Obraz dostarczany przez kamery cyfrowe jest analizowany na kilku poziomach przez sieć neuronową, co pozwala na jego pełne zbadanie. System bazuje na sygnałach z kamer pomiarowych i poglądowych.

Kamera pomiarowa ANPR/MMR umożliwia szczegółową identyfikację pojazdu. Wykrywa nie tylko jego numer rejestracyjny, ale także prędkość (chwilową, a przy zastosowaniu dwóch kamer również średnią), kierunek ruchu, markę, model, kolor. Ponadto potrafi określić typ pojazdu (wybiera go z następującej grupy: osobowy, dostawczy, ciężarowy, autobus, motocykl, inny).

Z kolei kamera poglądowa VLoop/Event służy do śledzenia obiektów (pojazdów), wykrywania nieprawidłowości w ruchu podczas zmiany fazy w sygnalizacji świetlnej (np. wykrywania pojazdów, które poruszają się na czerwonym świetle) oraz identyfikacji zdarzeń drogowych i wykroczeń.

System umożliwia identyfikację pojazdów i wykrywanie takich zdarzeń jak jazda pod prąd, jazda bez pasów bezpieczeństwa czy prowadzenie rozmowy przez telefon komórkowy podczas jazdy. Może być wykorzystywany na przykład w sieciach automatycznych punktów kontrolnych na granicach i drogach krajowych, w systemach parkingowych i systemach poboru opłat, a także w systemach kontroli dostępu do wyznaczonych stref.

APP, czyli Autonomiczne Punkty Pomiarowe bazujące na kamerach i promiennikach IR firmy Bosch, mogą między innymi kontrolować wagę pojazdów w ruchu i zapobiegać w ten sposób nadmiernemu niszczeniu nawierzchni na skutek ich przeciążenia. Potrafią wykryć pojazdy skradzione lub z innych powodów poszukiwane.

W systemach Neurocar wykorzystywane są dwa typy kamer Dinion 2× zgodnych z ONVIF – Bosch NBN-498 oraz NBN-921. Są to kamery dualne dzień/noc, których matryce mają bardzo dużą trwałość i umożliwiają wieloletnią pracę w różnych warunkach oświetleniowych i pogodowych bez konieczności serwisowania. Wykorzystanie kamer Dinion spowodowało, że linia systemów Neurocar 2.0 weszła do produktowej klasy premium.

W ciągu sekundy system Neurocar przetwarza 25 lub 30 klatek telewizyjnych o rozdzielczości 1024×760 pikseli. Wieloprocesowe oprogramowanie pozwala na równoległe przetwarzanie rejestrowanych obrazów. Detekcja obecności pojazdu następuje w czasie krótszym niż 12 ms, a rozpoznanie tablicy rejestracyjnej trwa około 40 ms.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

IX Zjazd Sprawozdawczo-Wyborczy i XX-lecie towarzyszenia POLALARM

16 listopada 2012 r. w Warszawskim Domu Technika NOT odbył się **IX Zjazd Sprawozdawczo-Wyborczy** stowarzyszenia **POLALARM**. **Bogdan Tatarowski**, od 20 lat do tej pory pełniący funkcję prezesa, otrzymał godność honorowego prezesa zarządu. Nowym prezesem zarządu stowarzyszenia został **Mirosław Prokocki**.

Z okazji jubileuszu **XX-lecia istnienia POLALARMU** odbyła się sesja jubileuszowa z udziałem członków stowarzyszenia i zaproszonych gości. Z tej okazji najbardziej zasłużeni członkowie zostali wyróżnieni medalami i honorowymi odznakami NOT, honorowymi odznakami KIG, honorowymi odznakami stowarzyszenia oraz dyplomami z okazji jubileuszu.

Członkowie-założycie POLALARMU, którzy spotkali się na założycielskim zjeździe w dniu 7 listopada 1992 r., to grupa pasjonatów i entuzjastów rozwoju młodej wtedy dziedziny, jaką były zabezpieczenia osób i mienia. Reprezentowali oni producentów, projektantów i instalatorów – stąd wzięła się pełna nazwa stowarzyszenia. Zjednoczyli się, by w nowych warunkach gospodarczych tworzyć branżę i reprezentować swoje interesy zawodowe.

W 1994 roku, jako samorząd naukowo-techniczny, stowarzyszenie zostało członkiem Federacji Stowarzyszeń Naukowo-Technicznych NOT, a w 1996 roku, jako samorząd zawodowy – członkiem Krajowej Izby Gospodarczej. Jako członkowie obu organizacji przywiązujemy ogromną wagę do dbałości o wysoki poziom techniki, usług, do etyki i wiarygodności zawodowej reprezentowanych przez nas firm.

Skupiliśmy w swoim gronie wybitnych fachowców. Chcieliśmy wyznaczać kierunki rozwoju branży oraz popularyzować wiedzę fachową. Byliśmy organizatorami Forum Monitoringu Polskiego, konkursu *Polski Mistrz Techniki Alarmowej, Konferencji Zarządzania Bezpieczeństwem Obiektów i Informacji,* a wcześniej *Konferencji Ogólnotechnicznej Systemów Zabezpieczeń Alarmowych* i konferencji odbywających się podczas targów SECUREX.

Obecnie członkami stowarzyszenia są przede wszystkim właściciele i pracownicy firm projektowo-instalacyjnych, administratorzy systemów ochrony, przedstawiciele firm produkcyjnych i dystrybucyjnych. Jest też grupa osób reprezentujących działy techniczne w agencjach ochrony i monitoringu. Są wśród nas rzeczoznawcy systemów technicznego zabezpieczenia osób i mienia oraz zarządzania bezpieczeństwem.

Po dwudziestu latach działalności możemy powiedzieć, że nasz udział w tworzeniu branży technicznej ochrony osób i mienia był ogromny. Osiągnęliśmy to wyłącznie dzięki pracy społecznej. Zrealizowaliśmy wiele przedsięwzięć, nie tylko dla naszych członków, ale i dla całej branży zabezpieczeń.

Bezpośr. inf. Bożena Gozdowska
POLALARM

Jubileusz 55-lecia istnienia firmy

POLON-ALFA to prężnie rozwijająca się firma o wieloletniej tradycji. Początki działalności zakładu przypadają na połowę lat pięćdziesiątych ubiegłego wieku, kiedy to główną specjalnością przedsiębiorstwa były zaawansowane badania nad promieniowaniem jonizującym. Ich efektem było zaprojektowanie i wprowadzenie do produkcji wielu urządzeń służących do wykrywania i pomiaru promieniowania, ogólnie nazywanych aparaturą dozymetryczną.

POLON-ALFA jako pierwsza firma w Polsce i trzecia na świecie skonstruowała i wprowadziła do produkcji jonizacyjną czujkę przeznaczoną do wykrywania dymu. Z biegiem lat działalność firmy została ukierunkowana na systemy sygnalizacji pożarowej – POLON-ALFA stał się największym producentem takich systemów w naszym kraju.

Dynamiczny rozwój firmy i doświadczona kadra inżynierska sprawiają, że obecną działalność przedsiębiorstwa doskonale określa widniejące przy logo POLON-ALFA hasło: „Najnowsza technologia. Najwyższa jakość".

Firma już od 20 lat jest organizatorem Ogólnopolskich Warsztatów „Sygnalizacja i Automatyka Pożarowa SAP",

POLON-ALFA

w których uczestniczą specjaliści związani z szeroko rozumianą branżą zabezpieczeń. Tak było też i w tym roku. Świętując jubileusz 20-lecia warsztatów, postanowiono zorganizować także obchody 55-lecia istnienia zakładu. Z tej okazji zaproszono na uroczystą kolację gościa specjalnego – Cezarego Pazurę. Fantastyczny, trwający ponad godzinę monolog, często przeradzający się w dialog z żywo reagującą publicznością, był niewątpliwie godnym uświetnieniem tego święta.

Aby nasi goście otrzymali od firmy nie tylko „coś dla ducha", drugiego dnia warsztatów przygotowaliśmy „coś dla ciała". Na parkingu przed budynkiem głównym Centrum Kongresowo-Konferencyjnego „Magellan", na dużych niebieskich foliach, stało dziesięć samochodów osobowych. Chętni do zabawy zostali podzieleni na dziesięć drużyn. Dostali ubrania ochronne, narzędzia i… zaczęło się demolowanie owych aut. Nie było to jednak bezmyślne niszczenie – w tak drastyczny sposób powstawały niesamowicie interesujące, zupełnie nowe pojazdy. Wyobraźnia uczestników zabawy przerosła nasze najśmielsze oczekiwania. Śmiechu było przy tym co niemiara, a końcowy wyścig był dobrą zabawą zarówno dla uczestników, jak i oglądających.

Jeszcze raz dziękujemy wszystkim gościom, którzy uświetnili obchody naszego 55-lecia, życząc im i sobie, byśmy jeszcze nie raz w takim gronie i w dobrym zdrowiu mogli świętować kolejne jubileusze.

Bezpośr. inf. POLON-ALFA

Trzecia edycja warsztatów firmy Axis Communications

podsumowanie

14 listopada 2012 r. w Warszawie, w hotelu The Westin Warsaw, odbyła się kolejna edycja warsztatów szwedzkiej firmy **Axis Communications**. W spotkaniu udział wzięło ponad 90 osób, w tym przedstawiciele firm dystrybucyjnych, projektowych oraz instalacyjnych, które na co dzień korzystają z urządzeń Axis. Firmę Axis reprezentowali Agata Majkucińska, Jan Grusznic, Daniel Lesisz oraz Dominika Troost (Marketing & Communication Coordinator w regionie CEE) i Jindrich Svetnica (Technical Trainer w Czechach i Słowacji).

Organizatorzy zapoznali uczestników z nowymi produktami i usługami oferowanymi przez firmę Axis.

Agata Majkucińska (Key Account Manager), która rozpoczęła spotkanie, przekazała najważniejsze informacje dotyczące koncepcji i zakresu działalności firmy na rynku światowym oraz w Polsce. Poinformowała zebranych również o tym, że szwedzki producent kładzie duży nacisk na edukację. Organizuje dużo szkoleń mających różne formy – od Axis Communications Academy po warsztaty związane z nowo wprowadzanymi urządzeniami. Rozbudowuje sekcję strony internetowej związaną z edukacją, w której można znaleźć samouczki, przewodniki, materiały szkoleniowe, zakładkę *White Papers* oraz szereg narzędzi ułatwiających projektowanie systemów.

Strona WWW umożliwia uzyskanie bezpłatnej pomocy technicznej. W zakładce *Wsparcie* można złożyć wniosek z prośbą o pomoc techniczną. Możliwe jest też uzyskanie pomocy na czacie z inżynierem. Ponadto do dyspozycji klientów jest dział FAQ zawierający listę ponad czterystu pytań i odpowiedzi dotyczących oferowanych rozwiązań. Klienci Axisa często znajdują rozwiązanie swoich problemów po zapoznaniu się z FAQ.

Filary firmy to światowa sieć partnerów, wielość oferowanych urządzeń oraz światowy zasięg. Według raportu IMS Research firma Axis Communications zajmuje obecnie pierwsze miejsce na rynku kamer sieciowych, jak również pierwsze miejsce na całym rynku kamer dozorowych.

Jan T. Grusznic (Sales Engineer w Polsce), który jest zatrudniony w Axis od października br., zaprezentował między innymi następujące urządzenia:

1) Wideoserwer AXIS Q7411. Umożliwia on przetwarzanie 60 klatek na sekundę. Ma wiele możliwości kompresji obrazu (metody H.264 Baseline, Main Profile i Motion JPEG). Zapewnia wielostrumieniową transmisję wizji oraz dwukierunkową transmisję dźwięku.
2) Wideoserwer AXIS Q7424-R. Jest on przystosowany do pracy w trudnych warunkach środowiskowych, w zakresie temperatur od 40°C do 75°C i przy wilgotności względnej od 10 do 95% (bez kondensacji).
3) Kopułkowe kamery sieciowe PTZ Axis Q60-C z aktywnym chłodzeniem. Kamery te są przystosowane do pracy w bardzo wysokich temperaturach, dochodzących do 75°C, a także w środowisku mocno zapylonym. Mają wbudowany system kontroli temperatury z elementem Peltiera, który utrzymuje optymalną temperaturę wewnątrz obudowy kamery niezależnie od tego, czy na zewnątrz panuje silny mróz czy upał.
4) Przełącznik sieciowy AXIS T8605 Media Converter Switch. Jest on wyposażony w dwa gniazda SFP na moduły miniGIBIC, dwa interfejsy RJ-45 i dwa porty I/O.
5) AXIS P3384-V/-VE. Jest to stałopozycyjna kamera kopułkowa o rozdzielczości HDTV 720p, która wykorzystuje rozwiązania WDR Dynamic Capture oraz Lightfinder i jest przeznaczona do pracy w ekstremalnych warunkach oświetleniowych.
6) Stałopozycyjna kamera kopułkowa AXIS M3007 –PV/-P. Jest to jedna z czterech kamer z serii Axis M30 i pierwsza z funkcją panoramy i przetwornikiem o rozdzielczości pięć megapikseli, która może być montowana zarówno na ścianach, jak i na sufitach. Może być wykorzystana do obserwacji pomieszczeń o powierzchni dochodzącej do 670 m^2.
7) Seria dyskretnych kamer sieciowych Axis P12. Są to miniaturowe kamery pracujące w standardzie HDTV 720p, służące do dyskretnej obserwacji dozorowanych obszarów. Seria składa się z trzech modeli kamer: P1204, P1214 i P1214-E.

Pod hasłem „Inteligencja w kamerach" odbyła się kolejna prezentacja poprowadzona przez Jindricha Svetnicę. Przedstawił on oprogramowanie Axis Camera Application Platform, które umożliwia modyfikację właściwości kamer i wideoserwerów zgodnie z indywidualnymi wymaganiami użytkowników końcowych. Omówił działanie aplikacji TrueView People Counter, która obecnie stanowi jedno z najnowocześniejszych rozwiązań w dziedzinie liczenia osób przebywających na obszarze obserwowanym przez kamery. Zastosowano w niej najbardziej zaawansowane algorytmy służące do inteligentnej analizy obrazu. System TrueView People Counter jest instalowany w pamięci standardowych kamer sieciowych przeznaczonych do montażu sufitowego. Zliczanie osób przebywających w polu widzenia kamery lub przechodzących przez umowną linię graniczną odbywa się w sposób automatyczny. W wersji standardowej oprogramowania szerokość obszaru, na którym odbywa się zliczanie, wynosi około pięć metrów, zaś w wersji *light* obszar jest zawężony do dwóch metrów. Uzyskane dzięki aplikacji dane statystyczne mogą być wykorzystane do poprawy funkcjonowania placówek handlowych lub do usprawnienia ruchu pieszego na wybranych obszarach.

Ostatnim prelegentem był Mariusz Czarnecki z Zakładu Obsługi Systemu Monitoringu, który przedstawił koncepcję profesjonalnego przygotowania głównych założeń projektowych na przykładzie warszawskiego systemu monitoringu (ZOSM jest organizacją odpowiedzialną za rozbudowę i rozwój systemu monitoringu w stolicy i współpracuje między innymi z warszawskim Biurem Bezpieczeństwa i Zarządzania Kryzysowego, policją i strażą miejską). W ubiegłym roku system został wyposażony w wideoserwery Axis, które umożliwiły włączenie posiadanych urządzeń analogowych do systemu IP i powiększenie go o dodatkowe kamery sieciowe. Jednym z głównych kryteriów, które brano pod uwagę podczas wyboru sprzętu do systemu monitoringu wizyjnego stolicy, była jakość obrazu, zwłaszcza w nocy, a także uzyskanie wysokiej poklatkowości przy zachowaniu maksymalnej rozdzielczości. ZOSM przygotował stanowisko testowe, korzystając z własnej infrastruktury dla wstępnie wytypowanych urządzeń. Producenci sprzętu oferowali dostęp do wiedzy, urządzenia i asystę techniczną. Ważnym aspektem była również kompatybilność z istniejącym systemem, a także rozważanymi rozwiązaniami VMS. W testach najlepiej sprawdziły się urządzenia Axis Communications.

Ostatnia część warsztatów przebiegła pod hasłem „Praktyka czyni mistrza". Podzieleni na pięć zespołów uczestnicy wykonywali różne zadania. Każdy uczestnik mógł zdobyć nowe doświadczenia i utrwalić wiedzę o produktach firmy Axis.

Serdecznie zapraszamy do obejrzenia fotorelacji, która jest dostępna na stronie *http://www.zabezpieczenia.com.pl/fotogalerie*.

Ela Końka

Warsztaty projektowe firmy Bosch na Stadionie Narodowym

podsumowanie

25 października na największym polskim stadionie, Stadionie Narodowym, odbyły się **warsztaty projektowe** zorganizowane przez firmę **Bosch**.

Podczas spotkania zaproszeni goście (głównie projektanci i instalatorzy systemów zabezpieczeń) mogli zapoznać się z rozwiązaniami Boscha, które zastosowano na Stadionie Narodowym. Bosch dostarczył ponad siedem tysięcy głośników do dźwiękowego systemu ostrzegawczego. Stworzył także największy w Polsce i Europie system sygnalizacji pożarowej w obiekcie sportowym. System ten składa się z ponad dziesięciu tysięcy elementów przyłączonych do czternastu central pożarowych umiejscowionych w różnych punktach stadionu i stanowiących jedną sieć bezpieczeństwa.

Na spotkaniu omówiono także zagadnienia związane z projektowaniem systemów zabezpieczeń wykorzystujących najnowsze rozwiązania oferowane przez firmę Bosch Security Systems.

Gośćmi specjalnymi byli Dariusz Cygankiewicz, przedstawiciel firmy Merawex, który wygłosił referat pt. *Systemy zasilania stosowane w sygnalizacji pożarowej (SSP, DSO) oraz innych urządzeniach przeciwpożarowych (SWP, SKRDiC)*, oraz Stanisław Krzyżanowski z Narodowego Centrum Sportu, który opowiedział o trudnych zadaniach, jakich musieli podjąć się wykonawcy Stadionu Narodowego.

W czasie warsztatów wygłoszono następujące referaty:

1) *Wykorzystanie nowoczesnych technologii Bosch CCTV IP do budowy zaawansowanego systemu dozoru wizyjnego;*
2) *Zastosowanie platformy BIS (Building Integration System) do wizualizacji i zarządzania SKD oraz SSWiN;*
3) *Nowe rozwiązania w systemach kongresowych serii DCN w połączeniu z kamerami Bosch HD;*
4) *Instalacja SAP na Stadionie Narodowym w Warszawie – od projektu do realizacji;*
5) *Planning Tool – zaawansowane oprogramowanie ułatwiające projektowanie SAP;*
6) *Instalacja DSO na Stadionie Narodowym w Warszawie – od projektu do realizacji;*
7) *Nowa wersja oddalonego mikrofonu strażaka do stosowania w instalacjach DSO.*

Dzięki uprzejmości organizatorów uczestnicy warsztatów mieli okazję zwiedzić Stadion Narodowy.

Teresa Karczmarzyk

Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy

podsumowanie

W dniach 9–10 października 2012 w Hotelu Windsor w Jachrance odbyły się **Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy**, będące kontynuacją dotychczasowego Ogólnopolskiego Szkolenia Projektowego Schrack Seconet.

Zgodnie z wcześniejszymi zapowiedziami spotkanie miało przede wszystkim szkoleniowy charakter. W ciągu dwóch dni specjalistycznych, merytorycznych wykładów połączonych z praktycznymi warsztatami swoją wiedzę na temat zaawansowanych systemów bezpieczeństwa poszerzyło ponad 420 uczestników!

Podczas spotkań z najlepszymi ekspertami z branży słuchacze mieli okazję zapoznać się z najnowszymi wytycznymi dotyczącymi projektowania takich systemów jak SSP, DSO, BMS, SMS, CCTV, SKD, SUG, sterowania oddymianiem i wydzieleniami pożarowymi, a także sieci strukturalnych. Swoje referaty wygłosili m.in.: przedstawiciele Instytutu Techniki Budowlanej, przedstawiciele najlepszych, specjalistycznych uczelni (SGSP, Politechnika Warszawska, Politechnika Wrocławska) oraz niezależni specjaliści, zajmujący się problematyką systemów bezpieczeństwa.

Najważniejszym punktem imprezy była prezentacja „na żywo" procedury zadziałania wszystkich zintegrowanych systemów bezpieczeństwa podczas pożaru.

Po raz pierwszy w historii uczestnicy szkolenia mieli możliwość, nie tylko w głębszy i pełniejszy sposób zapoznać się ze specyfiką systemów bezpieczeństwa w kontekście ochrony przeciwpożarowej, ale także mogli w sposób praktyczny przekonać się, jak funkcjonują systemy we wzajemnej interakcji.

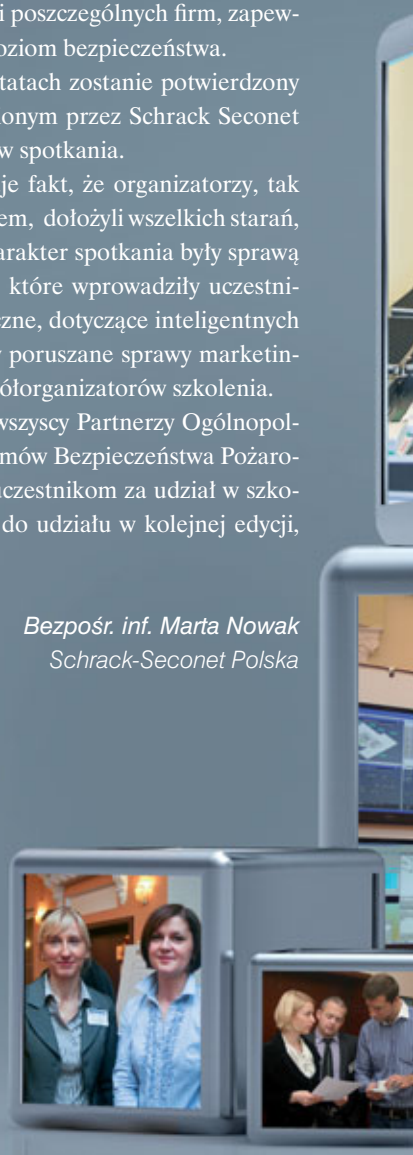
Do współorganizacji jedynego w branży zabezpieczeń szkolenia na tak dużą skalę zostali zaproszeni producenci innych systemów: Anixter Poland – wiodący, dostawca produktów komunikacyjnych, stanowiących podstawę systemów przesyłania dźwięku, video, danych i systemów zabezpieczeń; BELIMO – lider w produkcji napędów klap pożarowych oraz siłowników i zaworów przeznaczonych do instalacji HVAC; CommScope – opracowujący rozwiązania infrastruktury sieciowej; InGas – firma specjalizująca się w budowie urządzeń gaśniczych, gazowych; Johnson Controls International – czołowy dostawca produktów, usług oraz rozwiązań w zakresie systemów HVAC (chłodnictwa, wentylacji, klimatyzacji i ogrzewania), jak również Systemów Automatyki Budynkowej i BMS; Sony Europe – producent innowacyjnego sprzętu audio, wideo, telekomunikacyjnego i informatycznego, Display, CCTV; TOA Electronics Europe – lider na rynku systemów nagłośnieniowych, komunikacyjnych i bezpieczeństwa (DSO). W ciągu dwóch dni warsztatów, odbywających się równolegle w siedmiu salach, zrealizowano panele tematyczne poszczególnych producentów. Uczestnicy mogli poszerzyć swoja wiedzę m.in. o umiejętność projektowania poszczególnych systemów i zapoznać się z najnowszymi rozwiązaniami poszczególnych firm, zapewniających obiektom najwyższy poziom bezpieczeństwa.

Udział w dwudniowych warsztatach zostanie potwierdzony wspólnym certyfikatem, wystawionym przez Schrack Seconet Polska oraz wszystkich Partnerów spotkania.

Na szczególną uwagę zasługuje fakt, że organizatorzy, tak jak zapowiedzieli przed szkoleniem, dołożyli wszelkich starań, aby merytoryka i edukacyjny charakter spotkania były sprawą nadrzędną. W części referatów, które wprowadziły uczestników w najnowsze zmiany i wytyczne, dotyczące inteligentnych zabezpieczeń obiektów, nie były poruszane sprawy marketingowe poszczególnych firm – współorganizatorów szkolenia.

Firma Schrack Seconet oraz wszyscy Partnerzy Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego 2012 dziękują wszystkim uczestnikom za udział w szkoleniu, zapraszając jednocześnie do udziału w kolejnej edycji, w roku 2013.

Bezpośr. inf. Marta Nowak
Schrack-Seconet Polska



Redakcja *Zabezpieczeń* miała okazję uczestniczyć w wykładach i szkoleniach specjalistycznych odbywających się w ramach omawianych Dni. Najważniejszą informacją przekazaną uczestnikom przez prelegentów była naszym zdaniem pełna informacja o wejściu w życie z dniem 1 lipca 2013 roku Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 305/2011 z dnia 9 marca 2011 r., które ustanawiając zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych zmieni wiele przepisów związanych z bezpieczeństwem obiektów – rozporządzenie to wejdzie bowiem z mocą ustawy do naszego systemu prawnego bez jakichkolwiek pośrednich aktów prawnych. Wprawdzie rozporządzenie to dotyczy wyrobów budowlanych, ale pewne jego regulacje dotyczą obiektów i modyfikacji wymagań dla nich.

Z wymagań, które zaczną obowiązywać od 1 lipca 2013 wynika, że dla zapewnienia właściwego poziomu bezpieczeństwa i ochrony życia ludzi należy w większym niż dotychczas stopniu zastosować integrację i współdziałanie różnych systemów zabezpieczenia obiektu, czemu poświęcono najważniejsze wystąpienia, wykłady i warsztaty podczas dopiero co zakończonych Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego 2012.

Redakcja

Systemy sterowania i nadzoru szyte na miarę

Marcin Buczaj

W niniejszym artykule przedstawiam koncepcję budowy urządzeń sterujących współpracujących z mikrokomputerami klasy PC. W zarządzanym przez mikrokomputer układzie sterowania i nadzoru część decyzyjna systemu będzie zaimplementowana jako odrębna aplikacja, dopasowana do specyficznych wymagań użytkownika. Aplikacje zostaną stworzone w środowisku LabVIEW. Przedstawiona koncepcja umożliwia wykorzystanie dostępnych narzędzi programistycznych w tworzeniu zindywidualizowanych systemów sterowania i nadzoru. Ważny jest sposób interpretacji sygnałów pochodzących z elementów detekcyjnych systemu oraz możliwość przeniesienia procesu interpretacji wielkości rejestrowanego zaburzenia z detektora (czujki) do urządzenia sterującego i obrazującego systemu nadzoru. Artykuł ten w sposób ogólny przestawia koncepcję wirtualnych układów sterowania i nadzoru dla dozorowanych obiektów. Zawiera wprowadzające informacje dotyczące wirtualnych systemów sterowania i nadzoru wykorzystujących sprzęt mikrokomputerowy. Kolejne artykuły będą przedstawiały praktyczne rozwiązania z zakresu systemów alarmowych, zarządzania systemami monitoringu wizyjnego oraz układów sterowania i regulacji parametrów klimatycznych w pomieszczeniach

1. Wstęp

Zadania nowoczesnych systemów sterowania w budynkach nie ograniczają się już tylko do dostarczania energii elektrycznej o wymaganych parametrach. Obecnie wyspecjalizowane układy muszą kontrolować stan obiektu i sterować pracą zainstalowanych w nim urządzeń. W tym celu wyposaża się instalacje w układy sterujące umożliwiające realizację zamierzonych przez użytkownika funkcji i procedur, np. regulację działania oświetlenia, ogrzewania, wentylacji. W ten sposób możliwe jest zwiększenie komfortu użytkowania i podwyższenie poziomu bezpieczeństwa przy jednoczesnym ograniczeniu kosztów eksploatacji takich instalacji.

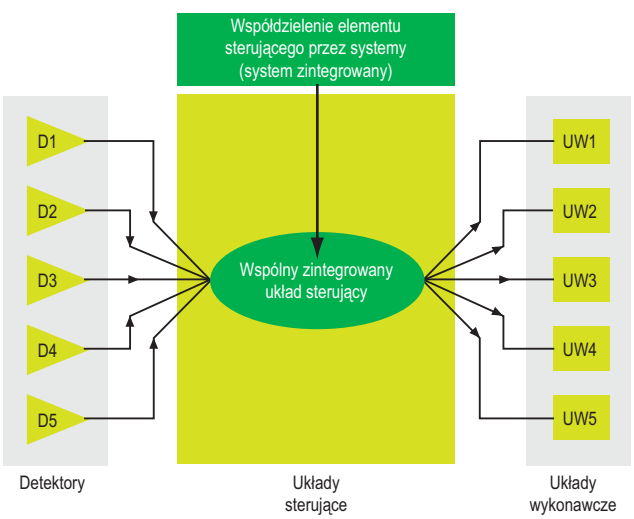
Proces integracji systemów sterowania i nadzoru polega na połączeniu poszczególnych, autonomicznych pod względem pełnionych w obiekcie funkcji, instalacji w jeden system realizujący wszystkie zadania poszczególnych jego części. Integracja autonomicznych systemów może odbywać się w następujący sposób:

– poprzez wymianę informacji pomiędzy autonomicznymi systemami,
– poprzez współdzielenie przez systemy elementów detekcyjnych i wykonawczych,
– poprzez realizację funkcji poszczególnych systemów przez jeden układ sterujący.

W przypadku systemów w pełni zintegrowanych pod względem sprzętowym i funkcyjnym (rys. 1) wszystkie elementy są przyłączone do jednego sterownika. Dzięki takiemu rozwiązaniu występuje tylko jeden układ nadzorujący, który ma dostęp do wszystkich informacji pochodzących z elementów detekcyjnych i według ustalonego programu pracy realizuje wyznaczone funkcje i steruje układami wykonawczymi systemu.

Obecnie jest wiele rodzajów systemów automatycznego sterowania pracą urządzeń, które nadają się do integracji sterowania i nadzoru. W budynkach mieszkalnych i gospodarczych najczęściej stosuje się:

– systemy oparte na magistrali EIB – stosowane w przypadku nowych instalacji i wykorzystywane przeważnie do regulowania parametrów klimatycznych i oświetleniowych, z opcjami zarządzania instalacjami alarmowymi [3],
– systemy ze sterownikami PLC – używane w przypadku adaptacji istniejącej instalacji do zadań integracyjnych, przeważnie do sterowania pojedynczymi układami urządzeń lub ich grupami [3],
– systemy wykorzystujące mikroprocesorowe sterowniki wbudowane – stosowane w podzespołach odpowiedzialnych za sterowanie poszczególnymi urządzeniami i w autonomicznych układach sterowania (np. centralach alarmowych),
– systemy z mikrokomputerami z zainstalowanym odpowiednim oprogramowaniem – charakteryzują się uniwersalnością i możliwością wykorzystania standardowych rozwiązań sprzętowych i programowych.

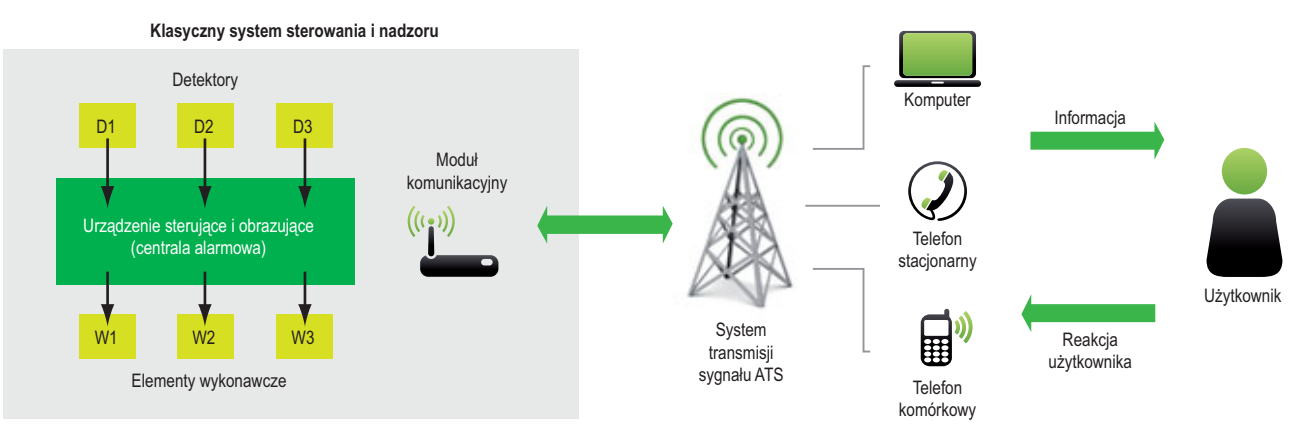


Rys. 1. System sterowania i nadzoru zintegrowany pod względem sprzętowym i funkcyjnym

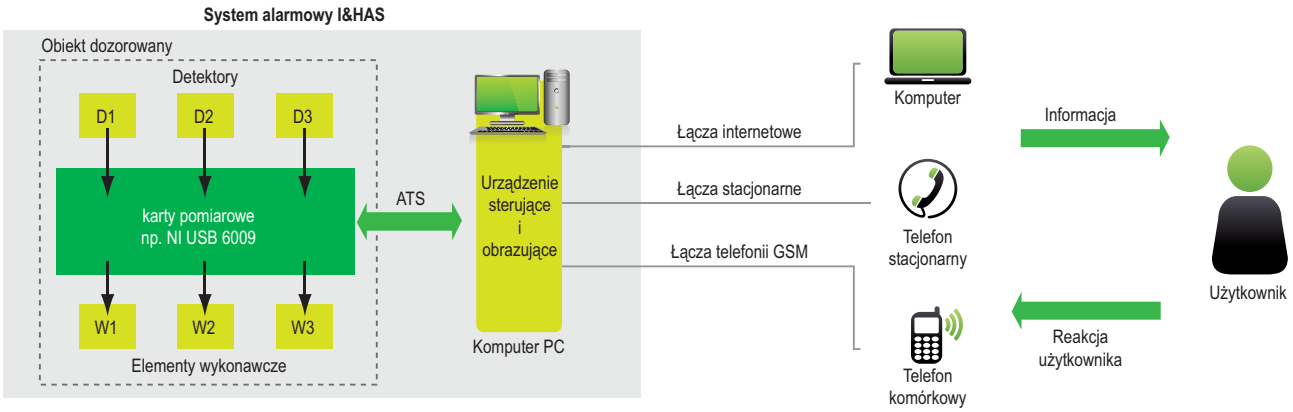
2. System nadzoru z klasycznym układem decyzyjnym

Klasyczny system nadzoru to układ zawierający urządzenie sterujące i obrazujące (np. centralę alarmową), elementy detekcyjne i wykonawcze oraz elementy odpowiedzialne za komunikację pomiędzy systemem a użytkownikiem. System nadzoru to „mózg" całego systemu alarmowego decydujący o uruchomieniu procedur wykonawczych. W tym układzie przechowywane są informacje o stanie wszystkich urządzeń współpracujących w danym systemie alarmowym, a wszystkie decyzje podejmowane są zgodnie z procedurami i algorytmami w programie sterującym.

Na rys. 2 został przedstawiony schemat organizacyjny systemu alarmowego I&HAS z klasycznym układem sterowania i nadzoru.



Rys. 2. Schemat organizacyjny klasycznego systemu sterowania i nadzoru



Rys. 3. Schemat organizacyjny systemu nadzoru z wirtualnym układem sterowania

Najważniejszym elementem systemu nadzoru jest urządzenie sterujące i obrazujące. Jego zadania [1, 6] to:

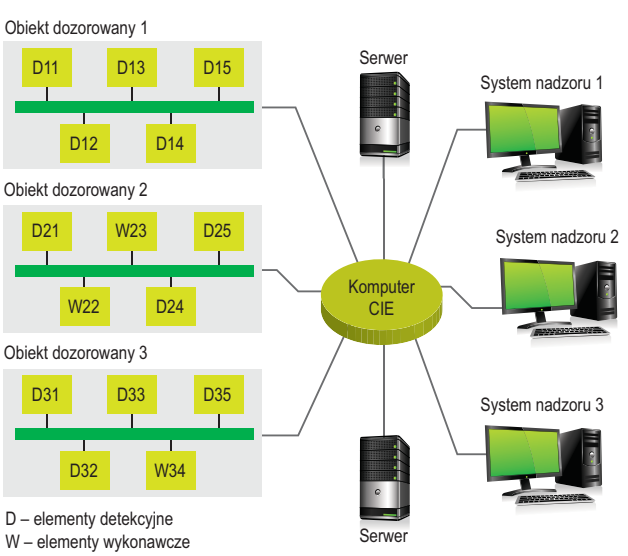
– odbieranie i przetwarzanie (zgodnie z programem sterującym) sygnałów informacyjnych (analogowych i/lub cyfrowych) z urządzeń zewnętrznych,
– sterowanie poprzez podanie odpowiednich sygnałów wyjściowych,
– obrazowanie zaistniałych zdarzeń na odpowiednich urządzeniach,
– transmisja informacji do innych systemów, np. alarmowego centrum odbiorczego (w skrócie ARC, ang. *alarm receiving centre*).

Cechą klasycznych układów jest to, że całość niezbędnej do prawidłowego działania systemu infrastruktury jest umieszczona w chronionym obiekcie. Ponadto układy odpowiedzialne za sterowanie pracą systemu nadzoru (np. central alarmowych) są fizycznie odseparowane od układów rejestrujących zaburzenia (np. czujek) oraz układów komunikacyjnych przekazujących użytkownikowi informacje o stanie systemu. Wymiana informacji pomiędzy podsystemami większych systemów nadzoru odbywa się na poziomie układów komunikacyjnych i central alarmowych. Podsystemy większych układów nie mają informacji o stanie elementu detekcyjnego, o ile nie są z nim fizycznie połączone. Może to wpływać na czas reakcji na zagrożenie, prawidłowość podjętej decyzji oraz skuteczność całego procesu neutralizacji zagrożenia.

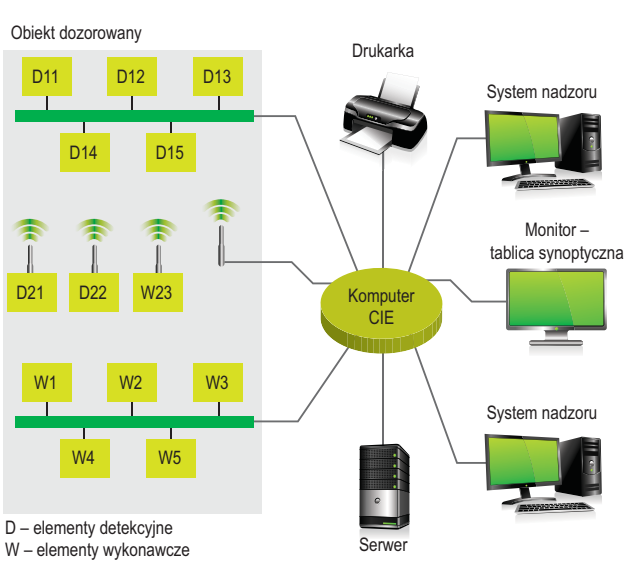
Elementy detekcyjne w klasycznym układzie systemu nadzoru działają zgodnie ze ściśle określonymi regułami progowymi. Po przekroczeniu ustalonego poziomu sygnału układ analizujący czujki przekazuje do centrali alarmowej tylko informację o zmianie stanu sygnału, nie przesyłając żadnej informacji o aktualnym poziomie zaburzenia. Wewnętrzne układy analizują poszczególne stany linii detekcyjnych, realizują założone funkcje i przekazują użytkownikowi informację o podjętych przez urządzenia sterujące decyzjach. Działanie klasycznych układów zarządzających pracą systemu alarmowego ogranicza się do realizacji funkcji logicznych uzupełnionych procedurami czasowymi.

3. System nadzoru wykorzystujący mikrokomputerowy układ sterowania

Koncepcja budowy mikrokomputerowego układu zarządzającego pracą systemu sterowania i nadzoru polega na zastąpieniu klasycznej centrali alarmowej, wyposażonej we wbudowany mikroprocesor, komputerem klasy PC (o budowie klasycznej, np. desktop, albo specjalnej – mikrokomputer, np. Raspberry Pi) z indywidualnie opracowaną (np. w programie LabVIEW) aplikacją sterującą. Z powodu braku możliwości obsługi dużej liczby elementów wejścia/wyjścia przez mikrokomputery to rozwiązanie techniczne wymaga wyposażenia układu zarządzania w dodatkowe moduły umożliwiające sprawdzanie stanów



Rys. 4. Topologia rozproszonego wirtualnego systemu nadzoru



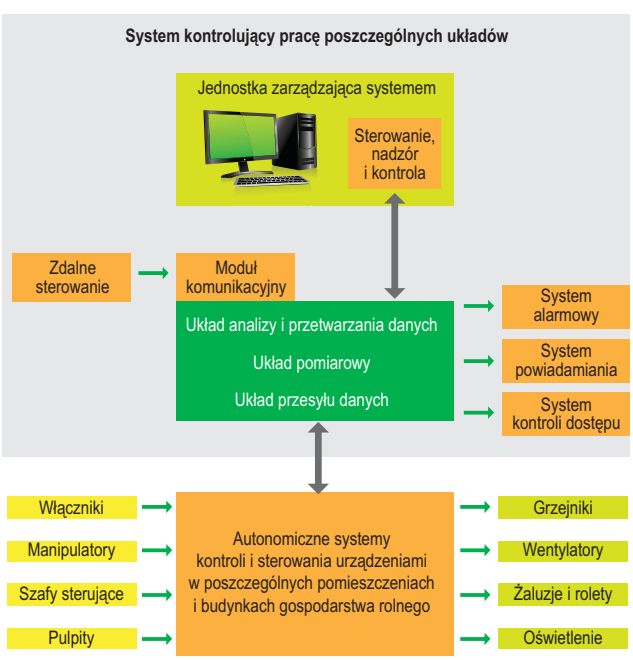
Rys. 5. Funkcjonalność wirtualnego systemu nadzoru

detektorów i wysterowywanie wejść elementów wykonawczych. Takimi modułami mogą być karty pomiarowe.

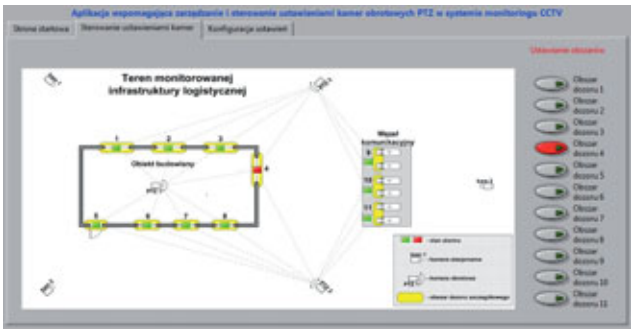
Powoduje to zmianę roli obwodów komunikacyjnych – z elementów peryferyjnych, przekazujących tylko informację o stanie systemu alarmowego przekształcają się w elementy istotne, równorzędne z obwodami sterującymi i detekcyjnymi. Dlatego ważne jest wyposażenie systemu alarmowego w odpowiedni, spełniający wymagania [2] system transmisji sygnału ATS. Kluczowym parametrem wpływającym na niezawodność działania systemu jest dostępność systemu transmisji, zróżnicowana w zależności od zadań realizowanych przez system nadzoru. Ze względu na konieczność transmisji sygnału ogólnodostępną siecią komunikacyjną ważna jest ochrona informacji transmitowanej.

Schemat organizacyjny systemu nadzoru z wirtualnym układem sterowania został przedstawiony na rys. 3. Taka organizacja systemu alarmowego umożliwia wyprowadzenie bloków analizująco-decyzyjnych z dozorowanego obiektu. Zastąpienie sprzętowych elementów służących do zbierania i analizy informacji elementami wirtualnymi (rys. 4) umożliwia budowę rozproszonych systemów analizująco-decyzyjnych o dowolnym stopniu powielenia. Utrudnia to sabotaż, praktyczne eliminuje możliwość ingerencji w proces działania rejestratora zdarzeń i uniemożliwia zniszczenie urządzenia sterującego podczas dokonywania włamania do obiektu [4].

Tworzenie wirtualnych komputerowych systemów pomiarowych [5], czasami nawet pracujących niezależnie, umożliwia ukierunkowanie ich na zróżnicowane traktowanie sygnału rejestrowanego przez detektory (rys. 5). System z analizą zaburzenia przeniesioną z elementów detekcyjnych do układu zarządzania (mikrokomputer i aplikacja sterująca) pozwala na opracowanie algorytmów wykorzystujących zmienne kryteria wywoływania stanu alarmu. Przesył całego nieprzetworzonego strumienia informacji źródłowej i jego zdalna analiza umożliwia zastosowanie



Rys. 6. Schemat organizacyjny komputerowego systemu sterowania i nadzoru



Rys. 7. Przykładowy interfejs użytkownika w programie LabVIEW

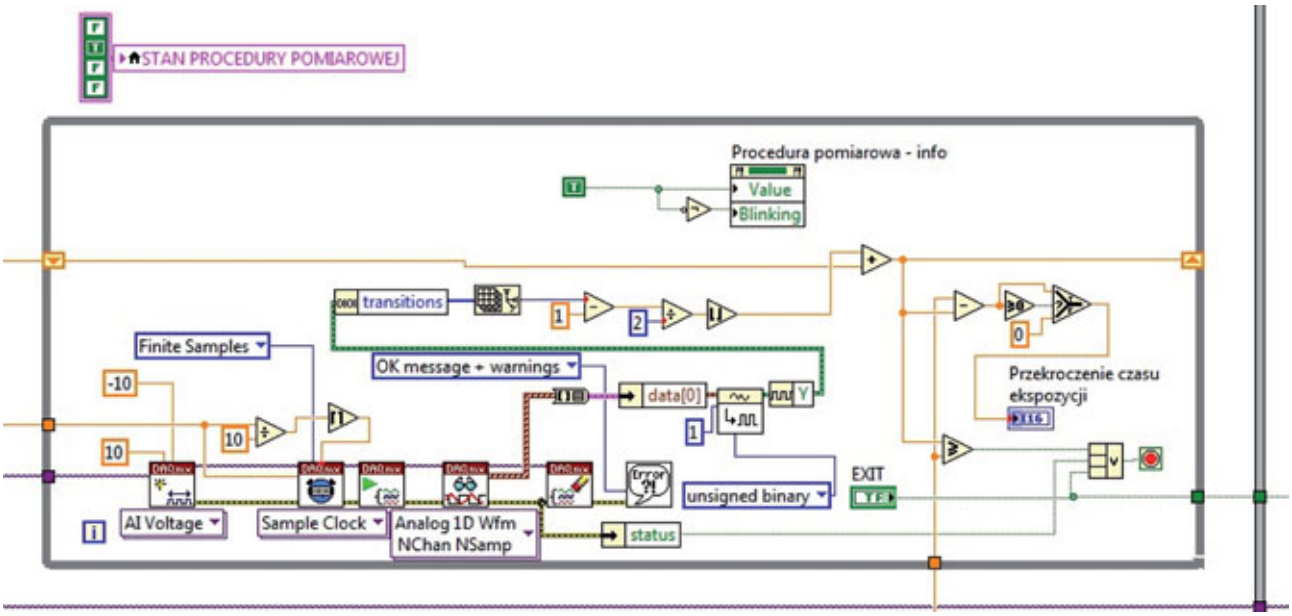
adaptacyjnych algorytmów wykrywania zagrożenia, dzięki którym kryteria oceny mogą się zmieniać w zależności od parametrów innych elementów detekcyjnych [4]. Takie rozwiązanie umożliwi wywołanie alarmu w przypadku niewielkiego zaburzenia wykrytego przez jedną z czujek i potwierdzenie tego zaburzenia również niewielkim pobudzeniem innej czujki. Nie jest to możliwe w przypadku klasycznego układu, gdy poziomy zaburzenia wywołujące alarm są ustawione na stałe i układ decyzyjny nie może określić aktualnych poziomów zaburzeń rejestrowanych przez poszczególne układy detekcyjne.

Głównym zadaniem projektowanego systemu nadzoru nad stanem infrastruktury w chronionym obiekcie jest umożliwienie użytkownikowi sprawowania kompleksowej kontroli parametrów bezpieczeństwa obiektu. Będzie to realizowane poprzez zbieranie przez system nadzoru danych pomiarowych z elementów detekcyjnych umieszczonych w poszczególnych strefach dozoru lub bezpośrednio z urządzeń stanowiących wyposażenie obiektu (parametry techniczne). Schemat blokowy organizacji wirtualnego systemu sterowania i nadzoru został przedstawiony na rys. 6.

4. Środowisko LabVIEW umożliwiające tworzenie aplikacji zarządzających pracą wirtualnych systemów sterowania i nadzoru

Aplikacja umożliwiająca sterowanie i kontrolę przez mikrokomputerowy system nadzoru kontrolujący stan chronionego obiektu została stworzona dzięki oprogramowaniu LabVIEW. LabVIEW umożliwia realizację złożonych funkcji gromadzenia, archiwizacji, przetwarzania i analizy danych pomiarowych. Dzięki temu można dowolnie kreować struktury programowe systemów pomiarowych i symulacyjnych, przydatnych w projektach naukowo-badawczych, a także tworzyć aplikacje umożliwiające budowę nowoczesnych systemów sterowania nadzorujących procesy technologiczne. LabVIEW umożliwia pomiary, sterowanie i zindywidualizowane tworzenie systemów obsługiwanych przez wielu użytkowników [5, 7, 8].

Stopnie dostępu poszczególnych użytkowników do systemu mogą być różne, zależne od uprawnień. Dzięki temu system jest stabilny i zabezpieczony przed nieuprawnionym dostępem. Dodatkową zaletą stworzonych w programie LabVIEW aplikacji jest ich oryginalność. Możliwe jest wykorzystanie zarówno gotowych schematów, jak i wyposażenie programów w indywidualne rozwiązania. Umożliwia to dopasowanie aplikacji do zmian w zabezpieczanym obiekcie



Rys. 8. Część schematu blokowego – procedura zbierania danych pomiarowych

(np. zmian architektonicznych, zmiany przeznaczenia poszczególnych pomieszczeń itp.).

W aplikacji zarządzającej i sterującej pracą systemu można wyróżnić następujące elementy:

– interfejs użytkownika (rys. 7) – umożliwia (w zależności od uprawnień) sterowanie, zmianę konfiguracji lub kontrolowanie pracy systemu,
– schemat organizacyjny (rys. 8) – schemat wewnętrznych powiązań poszczególnych elementów i aplikacji umożliwiających realizację zadań wyznaczonych przez użytkownika za pośrednictwem panelu sterującego,
– obsługa I/O (urządzeń wejścia i wyjścia) – część składowa systemu odpowiedzialna za wysyłanie informacji z elementów detekcyjnych systemu do urządzeń sterujących pracą elementów wykonawczych lub do użytkowników systemu.

Oprócz funkcji sterowania i kontroli stanu poszczególnych autonomicznych systemów sterowania komputerowy system nadzoru może mieć funkcję rejestracji zdarzeń.

5. Podsumowanie

Zintegrowane, zarządzane komputerowo systemy nadzorujące stan chronionego obiektu to rozwiązanie dające użytkownikowi wiele korzyści. Najważniejsze z nich to wymienność funkcji takich systemów oraz ich otwartość na modyfikacje. Dzięki zastosowaniu zintegrowanego systemu zarządzania instalacje domowe są pod nieustanną kontrolą, a użytkownik natychmiast otrzymuje informację o zmianie ich stanu. W przypadku awarii umożliwia to użytkownikom szybką lokalizację uszkodzenia i usunięcie źródła usterki.

Dzięki zastosowaniu oprogramowania LabVIEW firmy National Instruments użytkownik może mieć dostęp do zaawansowanych aplikacji umożliwiających komunikowanie się z urządzeniami zewnętrznymi na wiele sposobów. W takim systemie można wykorzystywać porty szeregowe i równoległe, protokół TCP/IP, łączyć się z urządzeniami bezprzewodowo.

Przeniesienie ośrodka oceny rodzaju i wielkości zaburzenia z elementów detekcyjnych (czujek) do układów sterujących, pełniących rolę central alarmowych umożliwia adaptacyjne ustalanie kryteriów wyzwolenia alarmów dla danych układów detekcyjnych na podstawie informacji o zaburzeniach w innych elementach detekcyjnych zainstalowanych w obiekcie. Umożliwia to także wykorzystanie w algorytmie sterowania funkcji arytmetycznych zamiast obecnie wykorzystywanych funkcji logicznych.

dr inż. Marcin Buczaj
Politechnika Lubelska
Katedra Inżynierii Komputerowej i Elektrycznej

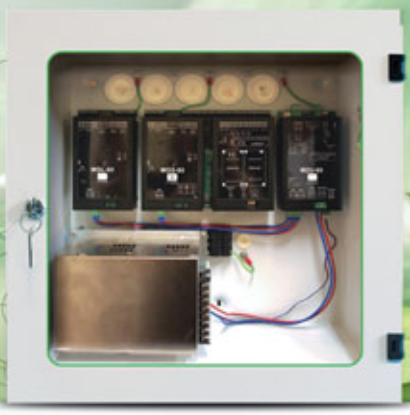
Literatura

1. PN-EN 50131-1 – *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe*, PKN, Warszawa 2009.
2. PN-EN 50136-1-1 – *Systemy alarmowe. Systemy i urządzenia transmisji alarmu. Wymagania ogólne dotyczące systemów transmisji alarmu,* PKN, Warszawa 2001.
3. Buczaj M., *Integracja systemów alarmowych i systemów zarządzających pracą urządzeń w budynku mieszkalnym, Zabezpieczenia* nr 4(68)/2009.
4. Buczaj M., *Wykorzystanie telefonii mobilnej i Internetu w procesie przekazywania informacji w systemach nadzorujących stan chronionego obiektu, Zabezpieczenia* nr 1(71)/2010.
5. Nawrocki W., *Komputerowe systemy pomiarowe*, WKiŁ, Warszawa, 2006.
6. Szulc W., Rosiński A., *Systemy sygnalizacji włamania. Część 1 – konfiguracje central alarmowych, Zabezpieczenia* nr 2(66)/2009.
7. Tłaczała W., *Środowisko LabView w eksperymencie wspomaganym komputerowo*, WNT, Warszawa 2002.
8. Chruściel M., *LabView w praktyce*, Wydawnictwo BTC, Legionowo 2008.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

UCS 6000

UNIWERSALNA CENTRALA STERUJĄCA



WEJŚCIA	UCS 6000	WYJŚCIA
• **praca samodzielna** czujki przyciski oddymiania		• **sterowanie 24 V** klapy z siłownikami dwukierunkowymi 2 lub 3 przewodowymi klapy z siłownikami ze sprężyną sterowanie elektrotrzymaczami itp.
• **praca jako element adresowalny w systemie POLON 4000**		
czujnik deszczu i/lub wiatru przyciski przewietrzające	• ponad 20 wersji • niemal dowolna konfiguracja • dedykowany program konfiguracyjny • 5 lat gwarancji	• **sterowanie 230 V~** wentylatory, kurtyny itp.

WSPÓŁPRACA Z CENTRALAMI SYGNALIZACJI POŻAROWEJ WSZYSTKICH PRODUCENTÓW

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

85-861 Bydgoszcz, ul. Glinki 155, www.polon-alfa.pl

Zintegrowany system interkomowy IP Pulse AlphaCom

Wojciech Wybraniec

Pulse AlphaCom to system interkomowy bazujący na technologii IP, który sprawdzi się wszędzie tam, gdzie wymagania dotyczące bezpieczeństwa są duże, np. w bankach, na lotniskach, w więzieniach, szpitalach i obiektach przemysłowych. Urządzenia końcowe mogą pracować w trzech trybach: jako urządzenia SIP z dowolnym serwerem telekomunikacyjnym obsługującym protokół SIP, jako elementy niewielkiego systemu Pulse, który nie wymaga zastosowania dedykowanego serwera, lub jako elementy systemu AlphaCom wyposażonego w zaawansowany serwer interkomowy

Wyjaśniając podstawowe różnice pomiędzy trybem Pulse a trybem AlphaCom, należy zwrócić uwagę na wielkość, funkcje oraz możliwości integracji systemu.

Pulse to rozwiązanie unikatowe w skali całego świata. System składa się wyłącznie ze stacji interkomowych i głośników IP, przy czym jedna z tych stacji pełni rolę serwera. Liczba urządzeń IP jest ograniczona do szesnastu. Mogą one realizować funkcje połączeń indywidualnych, grupowych i automatycznej odpowiedzi czy też sterować wyjściami przekaźnikowymi. Zakup dodatkowej licencji umożliwia podłączenie systemu do lokalnej centrali PBX lub sieci telefonicznej. W rezultacie rozwiązanie to nie wymusza na inwestorze zakupu serwera. Pulse daje możliwość płynnej migracji pomiędzy dostępnymi rozwiązaniami IP, między innymi przejścia do systemu AlphaCom.

Z kolei AlphaCom stanowi system o bardzo zaawansowanych funkcjach umożliwiających tworzenie sieciowych połączeń pomiędzy centralami, nagrywanie rozmów, realizację telekonferencji w trybie Duplex lub PTT, czy też odtwarzanie nagranych komunikatów głosowych z zachowaniem pełnej redundancji. Ponadto producent przewidział bardzo wiele

Fot. 1. Kolumna INFO SOS na stacji kolejowej SKM w Trójmieście

Fot. 2. Tryby pracy stacji interkomowych IP Stentofon

możliwości integracji – z innymi systemami łączności (z centralami analogowymi, GSM, ISDN, SIP, systemami DECT, systemami nagłośnienia PA), z systemami bezpieczeństwa, z systemami CCTV i KD – oraz obsługę otwartych protokołów, tj. OPC server, Microsoft .NET i SNMP. Producent opracował również system wizualizacji, to znaczy system graficznej reprezentacji aktualnego stanu każdego z urządzeń z możliwością nawiązywania połączeń bezpośrednio z tego systemu. Możliwa jest także reakcja na zdarzenia występujące w systemie – wykonanie zaprogramowanych poleceń lub sterowanie przekaźnikami i modułami wejścia/wyjścia.

Z punktu widzenia użytkownika istotne jest przede wszystkim uzyskanie niezawodnej komunikacji głosowej. Dzięki implementacji kodeka G.722 i nowoczesnych algorytmów analizy i przetwarzania sygnałów akustycznych oraz dzięki użyciu obudowy o specjalnej konstrukcji sprzęt zapewnia znakomite parametry akustyczne, co przekłada się na duży komfort rozmów prowadzonych za jego pośrednictwem.

Poniżej opisano kilka rozwiązań wartych uwagi.

Aktywna redukcja hałasu

Aktywna redukcja hałasu jest realizowana z użyciem programowego algorytmu zaimplementowanego w stacjach IP STENTOFON. Wydajny procesor DSP analizuje sygnał z mikrofonu, wyznacza poziom hałasu w tym sygnale i bardzo efektywnie usuwa część stanowiącą hałas, pozostawiając czyste dźwięki mowy, nawet gdy poziom sygnału mowy znajduje się znacznie poniżej poziomu hałasu pochodzącego z otoczenia. Ta funkcja znacznie ułatwia zrozumienie treści rozmowy prowadzonej w warunkach silnego hałasu związanego z ruchem ulicznym, na przykład przez interkomy parkingowe czy interkomy służące do wzywania pomocy na stacjach kolejowych. Istnieje możliwość regulacji poziomu filtracji hałasu w zakresie od 0 do 36 dB.

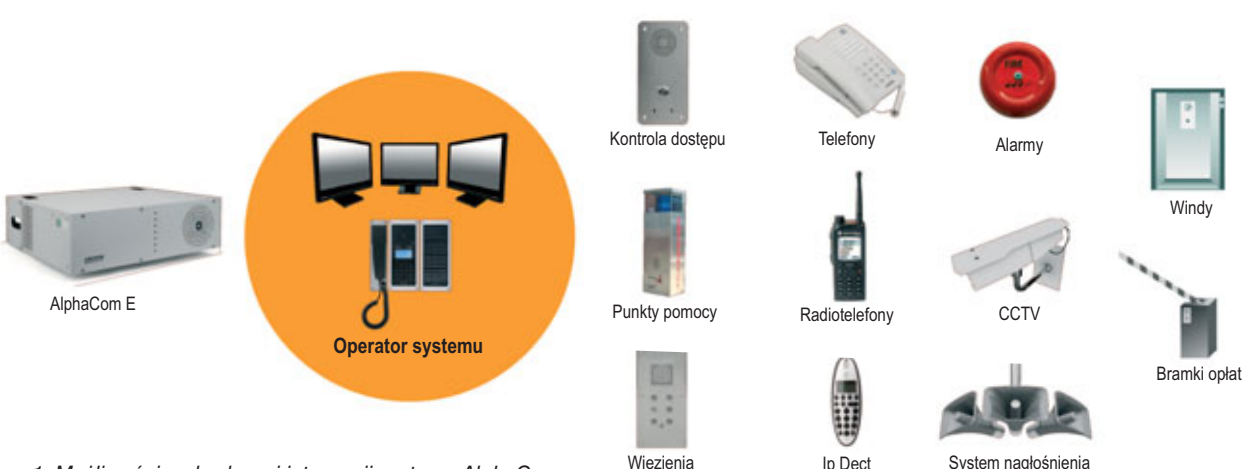
Automatyczna detekcja i analiza dźwięków

W listopadzie 2011 roku inżynierowie pracujący w firmach Zenitel AS oraz Audio Analytic zaimplementowali opcjonalne oprogramowanie CoreLogger w systemie interkomowym AlphaCom. W ten sposób stworzony został system bezpieczeństwa mający niespotykane dotychczas funkcje.

Ta unikatowa i innowacyjna integracja techniki dźwiękowej w systemie AlphaCom IP pozwala automatycznie powiadamiać o kradzieżach samochodów, włamaniach, napadach, aktach agresji poprzez wykrycie dźwięku alarmu samochodowego, dźwięku rozbitego szkła, podniesionego tonu głosu, krzyku towarzyszącego aktom agresji, odgłosu wystrzału z broni palnej. Można ustawić poziomy czułości odpowiadające wykrywaniu zdarzeń i parametry systemu. Operator może skupić się na najważniejszych faktach, informacjach i alarmach. Rozwiązanie to może znakomicie wspomagać istniejące systemy monitoringu wizyjnego, gdzie zastosowanie samych kamer nie zawsze wystarcza.

Nowoczesna konstrukcja i przetwarzanie sygnału mowy

Targi SECUREX 2012 były miejscem polskiej premiery najnowszych stacji interkomowych TURBINE. Niespotykane parametry akustyczne, doskonała zrozumiałość mowy, wysoki poziom ciśnienia akustycznego, zastosowanie wzmacniacza klasy D o mocy 10 W, wysoki stopień zabezpieczenia przed wnikaniem ciał stałych i wody (IP66) oraz stopień zabezpieczenia mechanicznego IK08 lub IK10 to tylko niektóre cechy



Rys. 1. Możliwości rozbudowy i integracji systemu AlphaCom

wyróżniające stację TURBINE. Specjalna konstrukcja głośnika zapobiega powstawaniu pogłosu i zmniejsza poziom zniekształceń. Stacje TURBINE automatycznie regulują swój poziom głośności, to znaczy ustawiają odpowiedni poziom wzmocnienia w zależności od tego, czy w otoczeniu mikrofonu panuje hałas, jaki jest wytwarzany przez silnik odrzutowego samolotu, czy tylko hałasuje przejeżdżający obok wózek bagażowy. Jednocześnie, dzięki wspomnianej wcześniej funkcji aktywnej redukcji hałasu, treść rozmowy prowadzonej przy takiej stacji może być zrozumiała pomimo zagłuszającego ją hałasu. Z kolei automatyczna regulacja wzmocnienia zapewnia ten sam poziom głośności niezależnie od tego, czy mówca znajduje się bardzo blisko, czy w odległości dochodzącej do siedmiu metrów od mikrofonu. W opisywanym interkomie zastosowano cyfrowy mikrofon MEMS, który charakteryzuje się dużą odpornością na zakłócenia elektromagnetyczne, ma płaską charakterystykę amplitudową i może pracować w szerokim zakresie temperatur. Implementacja algorytmów AEC (*acoustic echo cancellation*) w oprogramowaniu stacji TURBINE prowadzi do usunięcia pogłosu i zapobiega sprzężeniom w trakcie połączeń w trybie Open Duplex, gdy aktywne są głośniki i mikrofony w obu stacjach. Stacja TURBINE może pracować w trybie Open Duplex przy głośności dochodzącej do 95 dB! Obudowa tej stacji jest zabezpieczona przed aktami wandalizmu. Przyciski są podświetlane diodami LED w zależności od stanu połączenia. Producent przewidział również gniazdo służące do podłączenia pętli indukcyjnej wykorzystywanej przez osoby niedosłyszące. Wygląd zewnętrzny stacji TURBINE może być dostosowany do indywidualnych wymagań inwestorów. Na panelu frontowym może zostać nadrukowana dowolna grafika, logo organizacji lub inny wzór zwiększający walory estetyczne stacji, a także prestiż obiektu i rozpoznawalność organizacji.

Redundancja i niezawodność

Aktualnie system interkomowy AlphaCom może pracować z zachowaniem pełnej redundancji, co osiąga się dzięki zastosowaniu drugiego serwera pełniącego te same funkcje co serwer główny. Dodatkowy serwer może być zlokalizowany w dowolnym miejscu i musi mieć dostęp do tej samej sieci co serwer główny. Ponadto wybrane stacje interkomowe posiadają dwa porty RJ 45 pełniące rolę interfejsów sieciowych. Tym samym stacja pełni rolę zarządzalnego przełącznika sieciowego.

Fot. 3. Nowoczesna konstrukcja i przetwarzanie sygnału mowy

Fot. 4. Turbine TCIS-6

Jeden z interfejsów może być wykorzystany do połączenia z siecią LAN, zaś drugi może posłużyć do podłączenia innego urządzenia, na przykład kamery sieciowej.

Firma Stentofon opracowała własny protokół komunikacyjny CCoIP, (*Critical Communication over IP*) stanowiący rozszerzenie klasycznego protokołu VoIP, który uwzględnia wszystkie potrzeby, jakie mogą zaistnieć w sytuacjach krytycznych. System AlphaCom wykorzystuje protokół CCoIP umożliwiający przesyłanie kluczowych informacji, takich jak głos i dane. Dzięki wbudowanym mechanizmom zabezpieczającym zapewnia wysoki stopień ochrony komunikacji w sieci IP. Do głównych zabezpieczeń należą: zabezpieczenie dostępu do funkcji służących do zarządzania systemem, oddzielny interfejs konfiguracyjny, wbudowany firewall, możliwość utworzenia połączenia V-LAN (IEEE 802.1Q) oraz kontrola dostępu do zasobów sieci (IEEE 802.1X).

W przypadku systemów łączności interkomowej SOS, w których stacje mogą być używane sporadycznie, szczególnie ważna jest pewność, że stacja będzie działać. Z tego względu system interkomowy AlphaCom firmy STENTOFON posiada zaimplementowany system monitorowania linii oraz system testowania tonowego. W momencie wykrycia braku połączenia między stacją interkomową a serwerem (na przykład na skutek przecięcia kabla, odłączenia stacji lub jej uszkodzenia) system monitorujący stan linii wysyła ostrzegawczą wiadomość tekstową do głównego dyspozytora. System testowania tonowego sprawdza, czy w stacji interkomowej działa zarówno mikrofon, jak i głośnik. Jeżeli przynajmniej jeden z tych elementów jest uszkodzony, wysyła ostrzegawczą wiadomość tekstową do głównego dyspozytora. W taki system wyposażone są wszystkie stacje głośnomówiące.

Oddziaływanie na środowisko i energooszczędność

Niebagatelną zaletą opisywanych systemów jest niskie zużycie energii elektrycznej niezbędnej do ich zasilania. Serwery oraz urządzenia sieciowe pobierają znacznie mniej energii niż tradycyjne systemy interkomowe. Przykładowo – serwer AlphaCom XE1 obsługujący 552 abonentów sieciowych pobiera prąd elektryczny o mocy równej zaledwie 4 W. Inną zaletą jest możliwość zdalnego serwisu oraz zarządzania systemem przez Internet.

Wojciech Wybraniec
Novatel

Visonic
A Tyco International Company

Zapomnij wszystko co wiesz o bezprzewodowych systemach alarmowych!

PowerG oficjalny zwycięzca konkursu Złoty Medal Securex 2012

System PowerG firmy Visonic na nowo definiuje możliwości bezprzewodowych systemów alarmowych.

Innowacyjny. Bezpieczny. Najlepszy.

Stosując system PowerG:

- dostarczasz klientom stabilny i łatwy w obsłudze system alarmowy
- oszczędzasz pieniądze dzięki szybkiej i bezproblemowej instalacji
- chronisz środowisko poprzez stosowanie urządzeń pracujących nawet 8 lat na jednej baterii

Wyłączny dystrybutor produktów Visonic w Polsce:

AAT

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Axis wprowadza do swojej oferty miniaturowe kamery HDTV przeznaczone do systemów dyskretnego dozoru wizyjnego

Agata Majkucińska

Fot. 1. Kamery AXIS P12 są funkcjonalne i bardzo dyskretne

Firma Axis Communications, światowy lider w dziedzinie wizyjnych systemów dozorowych, wprowadza na rynek nowe kamery sieciowe z serii AXIS P12. Konstrukcja tych kamer w sposób szczególny predysponuje je do użycia w przypadkach, w których konieczne jest zachowanie maksymalnej dyskrecji. Odpowiedni kształt i małe rozmiary tych kamer umożliwiają łatwe wkomponowanie ich w otoczenie, przez co mogą one znaleźć zastosowanie w zakamuflowanych systemach dozorowych instalowanych w sklepach, bankach i punktach kasowych, a także w obiektach zabytkowych, hotelach i biurach.

Innym, nie mniej istotnymi miejscami zastosowań kamer z serii AXIS P12 są bankomaty, automatyczne stacje benzynowe i bezobsługowe punkty sprzedaży detalicznej, czyli wszelkie miejsca, w których dokonuje się operacji za pomocą kart kredytowych. Zarejestrowane obrazy mogą zawierać metadane dotyczące przeprowadzanych operacji finansowych. Zakamuflowane kamery są w stanie wykryć zarówno próby instalacji urządzeń kopiujących dane z kart kredytowych, jak i próby dokonania oszustw finansowych. Wysoka jakość obrazu pozwoli wykorzystać zarejestrowane obrazy w celach dowodowych. Dzięki użyciu kamer z serii AXIS P12 czas niezbędny do przeprowadzenia śledztwa znacznie się skróci.

Bardzo cennymi właściwościami kamer z serii AXIS P12 są ich niewielkie rozmiary oraz bardzo mała średnica obiektywu. Dzięki temu kamery mogą być umieszczone nisko, na wysokości oczu ludzkich, co znakomicie poprawi rozpoznawalność obserwowanych przez nie osób. Nie wystąpi dość uciążliwa wada kamer instalowanych na wysokości sufitu polegająca na braku dobrej rozpoznawalności osób noszących kapelusze czy inne nakrycia głowy zasłaniające twarz. Niespotykana w konkurencyjnych produktach opcja obracania obrazu o dziewięćdziesiąt stopni umożliwia lepszą obserwację przejść przez drzwi, wejść do wind, korytarzy, klatek schodowych.

Kamery sieciowe z serii AXIS P12 składają się z dwóch oddzielnych części połączonych za pomocą kabla – urządzenia sterującego i miniaturowego czujnika optycznego. Oba te elementy mogą być od siebie oddalone nawet o osiem metrów. Jak twierdzi Erik Fränlid, dyrektor działu opracowującego nowe produkty w firmie Axis, zarówno małe rozmiary jak i unikatowy kształt tych kamer umożliwiają łatwe zamontowanie ich w różnych miejscach, w których wymagane jest ukrycie instalacji.

Wśród kamer z serii AXIS P12 można wyróżnić trzy modele. Dwa z nich, AXIS P1204 i AXIS P1214, mają obiektywy o bardzo małej średnicy, dzięki czemu doskonale nadają się do zakamuflowanego montażu wewnątrz pomieszczeń. Z kolei kamera AXIS P1214-E jest umieszczona w miniaturowej obudowie o klasie szczelności IP66 i może pracować w temperaturach z zakresu od -20°C do 50°C, więc można zamontować ją na zewnątrz budynku.

Jak już wspomniano, wszystkie te kamery składają się z dwóch części połączonych ze sobą za pomocą kabla. Człon optyczny zawiera obiektyw i matrycę światłoczułą, zaś w członie sterującym umieszczone są układy elektroniczne niezbędne do prawidłowej pracy kamery. W skład kompletu wchodzą dodatkowe akcesoria ułatwiające montaż obu członów w różnych warunkach.

Kamery z serii AXIS P12 mogą wytwarzać obraz w standardzie HDTV 720p z pełną poklatkowością, kompresowany metodą H.264 lub Motion JPEG, dzięki czemu znajdują wiele zastosowań w kamuflowanych systemach dozorowych. Mogą być zasilane za pośrednictwem kabla sieciowego lub z wykorzystaniem osobnego zasilacza. Mają też funkcję lokalnej rejestracji obrazów na kartach pamięci microSD lub mocroSDHC, a także mogą współpracować z sieciowymi rejestratorami NAS. Ponadto kamery z serii AXIS P12 mogą pracować w systemach wykorzystujących oprogramowanie AXIS Camera Application Platform z opcją inteligentnej analizy treści obrazów, co pozwala na wykrywanie pewnych wstępnie zdefiniowanych wydarzeń zachodzących w obserwowanej przestrzeni. Dzięki portom I/O można podłączyć dodatkowe urządzenia peryferyjne, dzięki czemu w systemie dozorowym wykorzystującym te kamery mogą być realizowane funkcje alarmowe.

Kamery z serii AXIS P12 są być obsługiwane przez wszystkie aplikacje wchodzące w skład największych światowych zasobów oprogramowania systemowego Axis Application Development Partner Program oraz oprogramowania AXIS Camera Station. Projektant systemów może wykorzystać wszystkie urządzenia zgodne ze standardami AXIS Camera Companion, Hosted Video i ONVIF, co pozwala na integrację sprzętu pochodzącego od różnych producentów.

Kamery z serii AXIS P12 będą dostępne w sprzedaży od października 2012. Zdjęcia przedstawiające wygląd zewnętrzny tych kamer i ich dane techniczne można znaleźć na stronie: *www.axis.com/corporate/press/press_material.htm?key=p12series.*

Agata Majkucińska
Axis Communications

Fot. 2. Kamera AXIS P12 może być ukryta za ścianą – potrzebny jest jedynie niewielki otwór na obiektyw. Obiektyw może też całkowicie wystawać ze ściany

Fot. 3. Kamera AXIS P12 może być ukryta za cienkim metalowym arkuszem, na przykład w drzwiach lub w obudowie bankomatu

Fot. 4. Kamery AXIS P12 są dostępne w wersjach przeznaczonych do montażu wewnątrz lub na zewnątrz budynków

Nowe sieciowe kamery HD firmy Samsung

Tim Biddulph

W następstwie pomyślnego debiutu kamer SNB-5001 o rozdzielczości 1,3 megapikseli, będących w sprzedaży od czerwca tego roku, firma Samsung wprowadziła na rynek nową linię niedrogich kamer IP o rozdzielczości HD

Wszystkie modele kamer są zgodne ze standardem ONVIF. Do kompresji obrazów wykorzystują metody H.264 i MJPEG, dzięki czemu możliwa jest jednoczesna transmisja obrazów różniących się jakością i liczbą klatek na sekundę, przeznaczonych dla różnych odbiorców. W efekcie, po uzyskaniu autoryzacji, wielu użytkowników może korzystać z obrazów pochodzących z tych samych kamer. Jakość zdalnie rejestrowanych strumieni wizyjnych umożliwia wykorzystanie ich jako materiału dowodowego w sądzie. Dzięki aplikacji Samsung iPOLIS możliwe jest przeglądanie obrazów na smartfonach.

Każda z kamer ma funkcję wykrywania zmian zachodzących jednocześnie w całym polu widzenia kamery, dzięki czemu próby sabotażu, na przykład przez zamalowanie obiektywu farbą lub przez odwrócenie całej kamery przodem do ściany, skutkują wywołaniem alarmu.

Spośród innych dostępnych funkcji należy wymienić detekcję ruchu w dwunastu zaprogramowanych obszarach, możliwość wydzielenia dwunastu zamaskowanych stref prywatności oraz możliwość zasilania kamer metodą PoE. Najnowsze modele mają także funkcję automatycznego przełączania z trybu dziennego na tryb nocny i odwrotnie, co znakomicie zwiększa przydatność obrazów generowanych przez te kamery do celów dozorowych. Wszystkie oferowane kamery stacjonarne i kopułkowe są kompatybilne z bezpłatnym oprogramowaniem NET-i-Viewer oraz mają wielojęzyczne menu, dostępne na stronie WWW służącej do ich programowania, co znacznie upraszcza czynności związane z konfigurowaniem systemów dozorowych.

Kamery LiteNet

Do najnowszych sieciowych kamer firmy Samsung należą następujące urządzenia linii LiteNet:

- SNB-5001 – kamera stacjonarna o rozdzielczości 1,3 Mpx,
- SND-5010 – płaska kamera kopułkowa o rozdzielczości 1,3 Mpx,
- SND-5011 – kamera kopułkowa o rozdzielczości 1,3 Mpx, z obiektywem o stałej ogniskowej równej 3 mm,
- SND-5061 – kamera kopułkowa o rozdzielczości 1,3 Mpx, z obiektywem typu *varifocal*, o ogniskowej zmieniającej się w zakresie od 3 mm do 8 mm,
- SNB-7001 – kamera stacjonarna o rozdzielczości 3 Mpx, pracująca w standardzie Full HD,
- SND-7011 – kamera kopułkowa o rozdzielczości 3 Mpx, pracująca w standardzie Full HD, z obiektywem o stałej ogniskowej równej 3 mm,
- SND-7061 – kamera kopułkowa o rozdzielczości 3 Mpx, pracująca w standardzie Full HD, z obiektywem typu *varifocal*, o ogniskowej zmieniającej się w zakresie od 3 mm do 8 mm.

Zainteresowanie klientów z całej Europy nowymi kamerami LineNet było bardzo duże. Z rozmów prowadzonych z instalatorami systemów dozorowych dowiedzieliśmy się, że zapotrzebowanie na kamery pracujące w standardzie Full HD, dostarczające materiału wizyjnego o jakości umożliwiającej wykorzystanie go jako dowodu sądowego będzie bardzo duże, o ile cena tych kamer będzie na odpowiednim poziomie. Cena tych kamer musi być dostatecznie niska. Wówczas zainteresują one projektantów systemów dozorowych instalowanych w biurach i sklepach detalicznych.

Fot. 1. Płaska kamera kopułkowa Samsung LiteNet o rozdzielczości 1,3 Mpx

Budowanie rejestratorów NVR „z klocków”

Nowe rejestratory sieciowe firmy Samsung mogą być „budowane z klocków”, to znaczy mogą być projektowane na zasadzie doboru składników spełniających obecne wymagania użytkowników końcowych, a później można je rozbudować, jeśli wymagania te ulegną zmianie.

Kompatybilny ze standardem ONVIF rejestrator SRN-1000 NVR jest wyposażony w dysk o pojemności 24 TB i można podłączyć do niego dwie dodatkowe stacje dysków eSATA o łącznej pojemności 24 TB. Możliwe jest połączenie wielu urządzeń SRN-1000 i stworzenie sieci, w której materiał wizyjny może być zapisywany tak, jak w zwykłym serwerze.

Użycie prostego arkusza kalkulacyjnego i uwzględnienie ogólnej liczby klatek wizyjnych rejestrowanych w ciągu sekundy oraz rozdzielczości obrazów z poszczególnych kamer umożliwia łatwe ustalenie liczby rejestratorów SRN-1000 potrzebnej do zrealizowania danego projektu.

Urządzenia SRN-1000 wykorzystują system operacyjny Linux, są w stanie rejestrować strumień danych o przepływności 100 MB/s, dokonują kompresji obrazów metodami H.264, MPEG-4 I MJPEG i są w pełni kompatybilne z oprogramowaniem Samsung Centralized Management Software, które – za pośrednictwem komputera PC lub urządzeń przenośnych, takich jak smartfony czy tablety – umożliwia dostęp do zarejestrowanych nagrań wszystkim użytkownikom znajdującym się w dowolnym miejscu na świecie.

Fot. 2. Sieciowa kamera szybkoobrotowa Samsung Full HD

Fot. 3. System modułowych rejestratorów wizyjnych firmy Samsung

Rejestratory SRN-1000 współpracują z kamerami megapikselowymi i kamerami HD produkowanymi przez firmę Samsung, a także z kamerami takich producentów jak AXIS, Panasonic czy Sony, które są kompatybilne ze standardem ONVIF.

Nasi inżynierowie włożyli wiele wysiłku w stworzenie tych „klocków" i postarali się o to, by były one jak najłatwiejsze w użyciu, nawet dla osób dysponujących niewielką wiedzą na temat sieciowych systemów dozorowych Na przykład każdy z ośmiu dysków HDD zainstalowanych w rejestratorze SRN-1000 jest automatycznie rozpoznawany i może być natychmiast wykorzystany do zapisu.

Podobnie jak w przypadku profesjonalnych urządzeń firmy Samsung, przeznaczonych do tworzenia rozległych wizyjnych systemów dozorowych, rejestrator SRN-1000 jest objęty trzyletnią gwarancją, a nabywca ma zapewnione pełne wsparcie techniczne.

Nowa szybkoobrotowa kamera PTZ o rozdzielczości HD, z obiektywem zmiennoogniskowym o krotności ×20

Porty lotnicze i morskie, parkingi, szkoły, duże centra handlowe, podjazdy pod stacje benzynowe, stadiony sportowe to zaledwie niektóre obiekty, na których operatorzy wizyjnych systemów dozorowych chcieliby dysponować kamerami szybkoobrotowymi PTZ z obiektywami zmiennoogniskowymi o krotności ×20. Właśnie takie cechy ma kamera sieciowa SNP-6200 pracująca w standardzie Full HD.

Kamera SNP-6200 wytwarza obrazy o rozdzielczości 2 megapikseli, które mogą stanowić materiał dowodowy dla sądu. Przetworniki tych kamer są skanowane metodą Progressive Scan, dzięki czemu wytwarzane przez nie obrazy mają wysoką rozdzielczość nawet w przypadku obserwacji szybko poruszających się pojazdów. Obrazy mogą być wyświetlane w formacie 16:9, typowym dla standardu Full HD 1080p.

Kamera SNP-6200 ma wiele cech, które docenią pracownicy służb ochrony. Na przykład może wytwarzać wiele strumieni wizyjnych z użyciem kompresji metodą H.264 albo MJPEG. Dzięki temu obrazy z każdej z kamer mogą być jednocześnie wykorzystywane w stacjonarnych systemach monitoringu pracujących w czasie rzeczywistym, zapisywane na kartach pamięci SD w urządzeniach ruchomych i wysyłane pocztą elektroniczną wraz z powiadomieniem o alarmie.

Kompatybilna ze standardem ONVIF kamera SNP-6200 ma zainstalowane darmowe oprogramowanie Intelligent Video Analysis (IVA), które może pełnić rolę elektronicznej pułapki. Oprogramowanie wykrywa przekraczanie umownych linii granicznych przez poruszające się obiekty, a także pozwala na stwierdzenie pojawienia się jakiegoś obiektu w polu widzenia kamery lub zniknięcia obiektu z pola jej widzenia.

Opracowana przez firmę Samsung technologia Smart Codec umożliwia realizację funkcji rozpoznawania twarzy ludzkich, a także pozwala na zwiększenie rozdzielczości obrazu we fragmentach, które mogą być interesujące dla pracowników służb ochrony. Dzięki temu można na przykład obserwować i rejestrować obrazy przejść przez drzwi lub innych obszarów, na których przewijają się ludzie, z maksymalną dostępną rozdzielczością, a jednocześnie obserwować i rejestrować obrazy pozostałych miejsc mniej dokładnie, co umożliwia znaczne zmniejszenie rozmiarów rejestrowanych plików oraz ograniczenie zapotrzebowania na pasmo sieciowe.

Do innych zalet kamer SNP-6200 należy między innymi duża dynamika toru wizyjnego, możliwość zasilania metodą PoE i możliwość lokalnego zapisu materiału wizyjnego na karcie SD. Ponadto kamera SNP-6200 jest w pełni kompatybilna z darmowym oprogramowaniem Net-i-Viewer firmy Samsung, które pozwala na zdalne sterowanie i zarządzanie zasobami wizyjnego systemu dozorowego za pośrednictwem komputera PC w dowolnym miejscu na świecie.

Firma Samsung wprowadziła na rynek również kamerę SNP-6200 H, która ma takie same właściwości jak kamera SNP-6200, a ponadto jest przystosowana do pracy w niekorzystnych warunkach środowiskowych, na przykład w temperaturach od -500C do +500C. Obudowa kamery SNP-6200 H ma klasę szczelności IP66. W jej wnętrzu zainstalowana jest dmuchawa i grzałka zapobiegająca kondensowaniu się pary wodnej na przezroczystej osłonie.

Kamery SNP-6200 i SNP-6200 H są oferowane wraz z bogatym wyposażeniem dodatkowym, takim jak uchwyty umożliwiające montaż na ścianie, suficie, w narożniku muru, na słupie i parapecie.

Krótki film prezentujący działanie kamery SNP-6200 H jest zamieszczony na stronie *www.samsungsecurity.co.uk/videolibrary.*

Certyfikat IK-10 dla kamer wandaloodpornych

Wszystkie oferowane przez firmę Samsung analogowe i sieciowe modele kamer wandaloodpornych mają certyfikat IK-10 wydany przez niezależną placówkę badawczą.

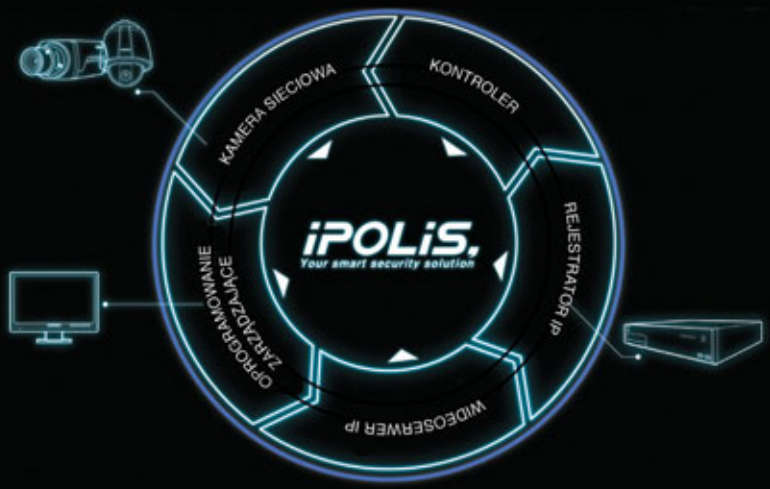
Firma EMC Compliance potwierdza, że wszystkie trzydzieści jeden przebadanych przez nią modeli kamer stacjonarnych i szybkoobrotowych firmy Samsung spełnia wymagania niezbędne do uzyskania certyfikatu IK-10 potwierdzającego ich odporność na udary mechaniczne (zgodnie z normami IEC 62262 i IEC 60068-2-75).

– Zaledwie kilku producentów poddało swoje wyroby rygorystycznym badaniom mającym na celu potwierdzenie zgodności ze standardami przemysłowymi obowiązującymi na terenie Europy. Nasi europejscy klienci mogą być pewni, że oferowane wandaloodporne kamery stacjonarne i obrotowe spełnią ich oczekiwania. W kamerach wykorzystaliśmy najnowsze, unikatowe rozwiązania technologiczne opracowane przez firmę Samsung, zaś ceny kamer są bardzo przystępne – powiedział Peter Ainsworth, Senior Product Manager firmy Samsung Techwin Europe.

Tim Biddulph
IP Product Manager firmy Samsung Techwin Europe

SAMSUNG

Wybierz SMART.
Wybierz inteligentne rozwiązania z zakresu zabezpieczeń!



Linia SAMSUNG iPOLiS oferuje inteligentne rozwiązania IP, idealnie dostosowane do Twoich potrzed. Doskonałej jakości urządzenia oferowane są z pełnym wsparciem przed- i posprzedażowym, w tym również w zakresie projektowania systemu i bezpłatnego wsparcia technicznego. Całość uzupełnia trzyletnia gwarancja na wszystkie produkty.

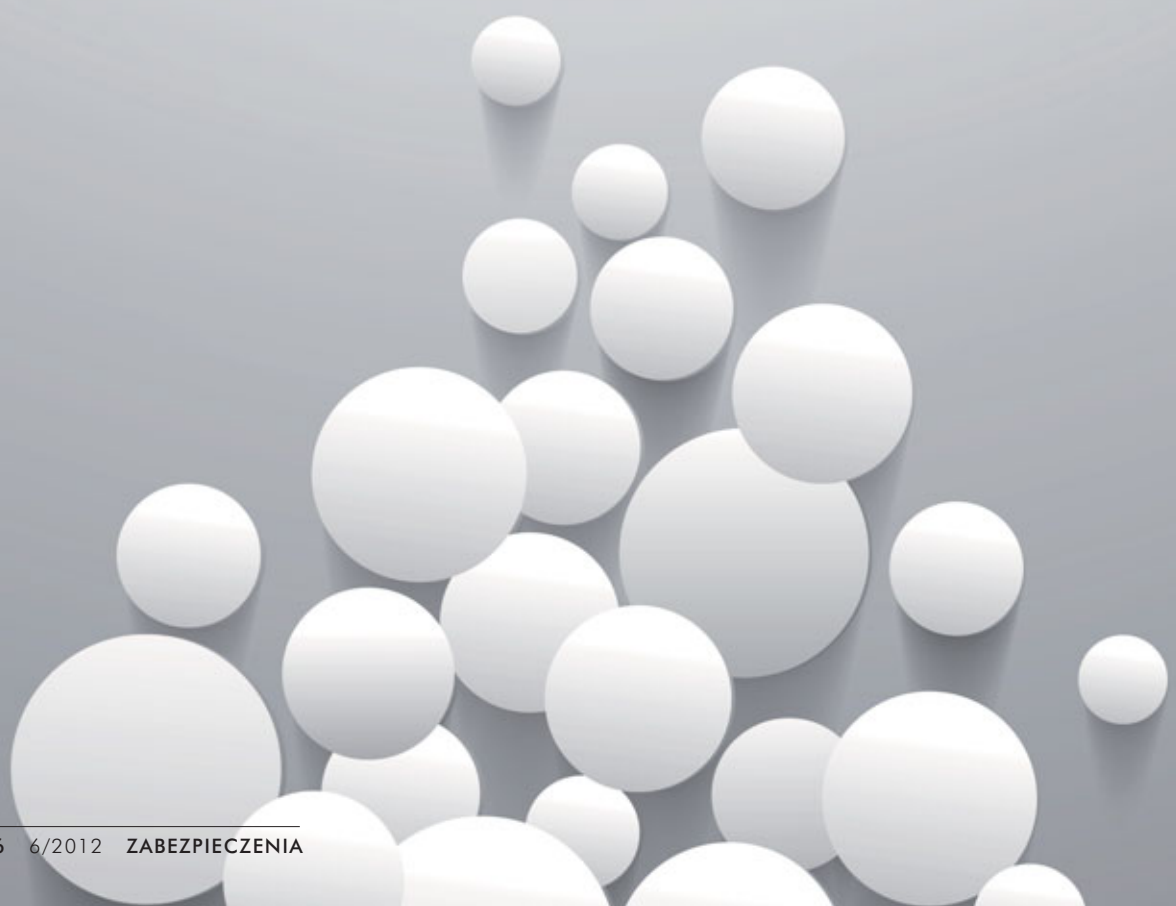
Samsung Techwin Europe Ltd

E STEsecurity@samsung.com
W samsungsecurity.com

Sieciowe kamery wizyjne Bosch Advantage Line z serii 200

Michał Biela

Bosch Security Systems wprowadził na rynek kolejne kamery z funkcjami przystosowanymi do zastosowań w małych i średnich instalacjach, mianowicie dwa modele profesjonalnych kamer o wysokiej rozdzielczości: model dwumegapikselowy NDC-274- PT oraz pięciomegapikselowy NDC-284-PT



Urządzenia te dostępne są bezpośrednio u dystrybutorów Advantage Line firmy Bosch. Nowe urządzenia należą do szerokiego asortymentu produktów oferowanych instalatorom specjalizującym się w małych i średnich sieciowych systemach dozorowych.

Obecnie na rynku dostępne są kamery o standardowej rozdzielczości, takie jak NBC-255 czy NDC-255, oraz modele o rozdzielczości HD: NBC-265 i NDC-265. Wraz z wprowadzeniem kamer NDC-274-PT oraz NDC-284-PT asortyment urządzeń IP został uzupełniony o modele o rozdzielczości Full HD.

Obrazy z kamer NDC-274-PT i NDC-284-PT mają doskonałą jakość, dzięki czemu możliwe jest wychwycenie drobnych szczegółów obserwowanych scen. Firma Bosch opracowała własną, zaawansowaną technologicznie wersję kompresji H.264 określaną jako H.264 Main Profile, dzięki której obrazy z kamer NDC-274-PT i NDC-284-PT stają się jeszcze bardziej czytelne.

Strumień danych wytwarzany przez kamery NDC-274-PT i NDC-284-PT może być zapisywany w pamięci umieszczonej wewnątrz każdej z kamer, w specjalnie do tego przeznaczonym gnieździe, lub może być rejestrowany w zewnętrznych urządzeniach pamięciowych ISCSI-NAS.

Dzięki wyrafinowanym funkcjom nowych kamer oraz wysokiej maksymalnej rozdzielczości obrazów, dochodzącej w przypadku modelu NDC-274-PT do 2 Mpix, a w przypadku modelu NDC-284-PT – do 5 Mpix, projektanci dostają do ręki narzędzia umożliwiające tworzenie funkcjonalnych systemów dozorowych.

Instalacja, obsługa i konserwacja kamer Bosch NDC-274-PT oraz NDC-284-PT jest łatwa. Użytkownicy tych kamer mają do dyspozycji trzy opcje zasilania: Power-over-Ethernet (PoE), 24 V_{AC} oraz 12 V_{DC}. Jednoczesne zasilanie kamer z dwóch niezależnych źródeł, to znaczy z sieci IP metodą PoE oraz z zasilacza 24 V_{AC} lub 12 V_{DC}, zwiększa niezawodność systemu.

Kamery IP z serii 200 mają oprogramowanie układowe zunifikowane z produktami ze standardowej oferty firmy Bosch. Koncepcja ujednolicenia oprogramowania układowego daje możliwość aktualizacji oprogramowania wszystkich kamer sieciowych z kompresją H.264 z wykorzystaniem tego samego pliku źródłowego. Wszystkie bieżące wersje firmware można bezpłatnie pobrać ze strony internetowej.

Na uwagę zasługują również parametry mechaniczne kamer. Oba modele wyróżniają się niezwykle małą, a zarazem wytrzymałą obudową. Kamery zostały przetestowane i spełniają wymagania wynikające z normy NF EN 50 102. Wytrzymują one udar mechaniczny o energii równej 5 J, co odpowiada odporności na uderzenie określanej w nomenklaturze technicznej jako IK08.

Ponadto kamera NDC-274-PM została wyposażona w złącze M12, które spełnia wymagania wynikające z normy EN 50155, dzięki czemu kamera może znaleźć zastosowanie w kolejnictwie i w transporcie drogowym.

Kamery megapikselowe Bosch serii IP 200 są sprzedawane w komplecie z zasilaczem, kartą pamięci 4 GB i bezpłatnym oprogramowaniem służącym do konfiguracji sprzętu.

Konfigurację sprzętu za pośrednictwem sieci IP ułatwia intuicyjny interfejs użytkownika. Takie rozwiązanie pozwala na stworzenie w pełni samodzielnego i funkcjonalnego punktu dozorowego bez konieczności budowania skomplikowanych sieci komputerowych.

W przypadku instalacji wykorzystujących wiele kamer dozorowych kompatybilność urządzeń jest jednym z warunków ich sprawnego działania. Wszystkie kamery Bosch serii IP 200 są zgodne z ONVIF (*Open Network Video Interface Forum*).

Do każdej kamery HD dodawane jest bezpłatne oprogramowanie Bosch Video Client Software, które umożliwia nie tylko instalację i konfigurację sprzętu, lecz także podgląd obrazu z wielu kamer na żywo, odtwarzanie i wyszukiwanie scen na potrzeby postępowania dowodowego oraz eksport danych. Dostępna jest również aplikacja, dzięki której możliwe jest wykorzystanie smartfonu lub tabletu do podglądu obrazów.

Urządzenia sieciowe Bosch Advantage Line z serii 200 umożliwiają tworzenie systemów dozorowych pracujących w trybie ciągłym, to znaczy przez siedem dni w tygodniu, dwadzieścia cztery godziny na dobę. Urządzenia te można zastosować w biurach, sklepach detalicznych, restauracjach, szkołach i innych obiektach użyteczności publicznej.

Nowe kamery Bosch IP serii 200 to oczywisty wybór dla każdego użytkownika, któremu zależy na cyfrowym systemie wizyjnym w przystępnej cenie.

Michał Biela
Bosch Security Systems

Systemy klucza generalnego

Mariusz Mikołajewski

Każdy z nas posiada klucz, a najczęściej pęk kluczy do mieszkania swojego, rodziców, biura itp. Oczywiście ważne jest to, by klucz był trudny do skopiowania, ale bardzo pożądaną cechą staje się również możliwość posługiwania się jednym kluczem do kilku różnych zamków

Renomowani producenci zamknięć oferują od wielu lat tzw. systemy klucza generalnego (ang. *master key systems*), które w języku polskim określane są również jako układy centralnego otwierania (taka terminologia użyta jest w Polskiej Normie PN-78/B-94461-07 dotyczącej takich rozwiązań). Wielu rodaków spotkało się już z takimi rozwiązaniami za granicą (szczególnie w Skandynawii i w Niemczech) – np. mogli jednym kluczem otworzyć wejście do budynku, drzwi do wspólnego pomieszczenia gospodarczego i drzwi wynajmowanego przez siebie mieszkania. W Europie Zachodniej takie rozwiązania są wykorzystywane od wielu dziesięcioleci.

W naszym kraju coraz więcej ludzi wie, że zamiast pękiem kluczy można posługiwać się kluczem generalnym, ale nie znaczy to, że wie o tym większość i że rozwiązanie to jest popularne. Pod tym względem wiele zmieniło się od lat 90. Pamiętam, że gdy w 1998 roku rozpoczynałem swoją pracę w branży zabezpieczeń, nie tylko użytkownicy indywidualni, ale i przedstawiciele inwestorów i dużych firm budowlanych dopiero ode mnie dowiadywali się, co to jest system klucza generalnego i na czym polega jego funkcjonalność. Obecnie sytuacja jest dużo lepsza – większość inwestorów i generalnych wykonawców wie, czym jest ten system, choć często nie są oni w stanie określić, jakiej funkcjonalności oczekują od tego rozwiązania w realizowanej przez siebie inwestycji.

Nadal wielu potencjalnych zainteresowanych nie wie, że nie musi używać pęku kluczy, jakie zalety ma stosowanie klucza generalnego, u kogo szukać fachowej porady i z jakimi kosztami to się wiąże. Jedno jest pewne: potencjalnych klientów, których stać na takie rozwiązanie, jest wielu. Niniejszy artykuł ma na celu obiektywne poinformowanie potencjalnych użytkowników, czym jest system klucza generalnego, dlaczego powinni rozważyć jego zastosowanie w domu lub firmie oraz na jakie parametry powinni zwrócić szczególną uwagę przed dokonaniem ostatecznego wyboru produktu.

Czym jest system klucza generalnego (SKG)?

Otóż SKG jest systemem kontroli dostępu do poszczególnych pomieszczeń, którego elementami wykonawczymi są wkładki bębenkowe, kłódki, zamki i inne rodzaje zamknięć oraz klucze.

W przypadku zastosowania zamknięć wykonanych w systemie klucza generalnego użytkownik posługuje się jednym kluczem i otwiera nim tylko drzwi do tych pomieszczeń, do których ma dostęp. W przypadku dobrych rozwiązań liczba możliwych do otworzenia jednym kluczem drzwi może być niemal nieograniczona.

Zastosowanie systemu klucza generalnego w domu/firmie zapewnia użytkownikowi:

a) kontrolę dostępu – każdy użytkownik otwiera swoim kluczem tylko te pomieszczenia, które powinien;
b) bezpieczeństwo:
   – klucze systemowe można dorobić tylko na podstawie karty bezpieczeństwa u dostawcy systemu (właściciel obiektu/systemu ma pełną kontrolę nad liczbą dorabianych kluczy);
   – zamki są wyposażone w dobre wkładki klasy bezpieczeństwa 6/2/C wg normy PN-EN1303:2007 (antywłamaniowe);
   – klucz awaryjny/przeciwpożarowy umożliwia szybką i sprawną ewakuację z budynku ludzi i wartościowego sprzętu, np. w przypadku wybuchu pożaru.
c) wygodę – każdy użytkownik posługuje się tylko jednym kluczem;
d) funkcjonalność – SKG może obejmować wszystkie rodzaje zamknięć na terenie domu/zakładu (wkładki, kłódki, cylindry, zamki przemysłowe itd.), a zainstalowany system można rozszerzać i modyfikować w przyszłości.

Zastosowanie systemu klucza generalnego

Systemy klucza generalnego można zastosować w domach jednorodzinnych, budynkach wielorodzinnych, małych firmach, biurowcach, fabrykach, centrach handlowych, hotelach, obiektach sportowych, urzędach, sądach, na uczelniach itp. Mogą z nich korzystać także duże firmy z sektora energetycznego, paliwowego, gazownictwa, telekomunikacji, wojsko oraz banki.

Wybierając SKG, należy sprawdzić, czy klucz jest powszechnie dostępny, zastrzeżony czy chroniony patentem (w Polsce). Wkładki w systemie powinny być certyfikowane (klasa zabezpieczenia klucza 6, klasa odporności na atak 2 i klasa odporności na włamanie C wg PN-EN1303:2007 oraz KT/402/IMP/2009). Wkładki powinny mieć klasę trwałości 6 wg PN-EN1303:2007 i wytrzymać 100 tysięcy otwarć i zamknięć). Wkładki zbudowane w systemie klucza generalnego powinny być zgodne z Polską Normą PN-78/B-94461-07. Wówczas można je stosować w układach centralnego otwierania. W promieniu dwustu kilometrów powinien być autoryzowany dystrybutor wybranego systemu, który zaprojektuje system klucza generalnego, dokona pomiarów długości wkładek w drzwiach, zamontuje system i otoczy go opieką serwisową zarówno w okresie gwarancyjnym, jak i pogwarancyjnym.

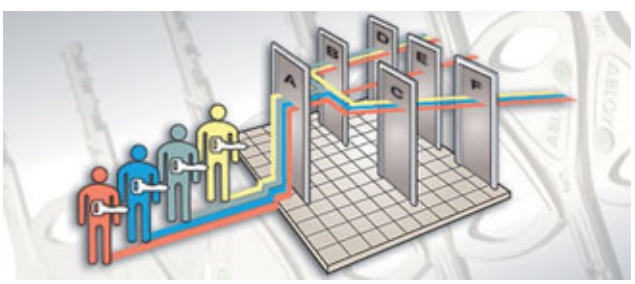
Dopasowanie systemu do obiektu

Spróbujmy określić, jak powinna wyglądać struktura dostępu w każdym z typów obiektów, w których miałby funkcjonować SKG, oraz jakie powinny być minimalne wymagania dotyczące systemu.

Dom jednorodzinny – system wkładek ujednoliconych

Zasada działania

Jeden klucz może być powielony w tylu egzemplarzach, ilu jest użytkowników. Otwiera wszystkie zamknięcia w domu, czyli np. furtkę, bramę wjazdową, bramę garażową, wejście główne do domu (z reguły są dwie wkładki w drzwiach), przejście pomiędzy domem a garażem, wiatkę ogrodniczą itd.



Rys. 1. Działanie systemu klucza generalnego

Minimalne wymagania dotyczące systemu

– zastrzeżony profil klucza (dorobienie klucza chronionego aktualnym patentem przez osoby nieuprawnione jest bardzo utrudnione, a w wielu przypadkach wręcz niemożliwe);
– certyfikat klasy 6/2/C wg PN-EN1303:2007 i KT/402/IMP/2009, wydany przez Instytut Mechaniki Precyzyjnej lub Instytut Techniki Budowlanej;
– lokalny serwis zapewniany przez autoryzowanego partnera producenta.

Budynek wielorodzinny/wspólnota mieszkaniowa – system wkładek centralnych

Zasada działania

Każdy z lokatorów używa jednego klucza, którym otwiera swoje mieszkanie, piwnicę, wejście na klatkę schodową przy domofonie, śmietnik itp. Żaden lokator nie może otworzyć mieszkania sąsiadów.

Minimalne wymagania dotyczące systemu

– zastrzeżony profil klucza;
– certyfikat klasy 6/2/C wg PN-EN1303:2007 i KT/402/IMP/2009, wydany przez Instytut Mechaniki Precyzyjnej lub Instytut Techniki Budowlanej;
– lokalny serwis zapewniany przez autoryzowanego partnera producenta.

Mała firma – system klucza grupowego

Zasada działania

Każdy z pracowników posługuje się jednym kluczem, którym otwiera swoje biuro, natomiast właściciel firmy/dyrektor swoim jednym kluczem otwiera wszystkie biura. Jeśli jest taka możliwość, klucz generalny otwierający wszystkie pomieszczenia może być zdeponowany w bezpiecznym miejscu u ochrony (np. w kopercie bezpiecznej w sejfie) i służyć jako klucz przeciwpożarowy umożliwiający ewakuację osób i wartościowego sprzętu w razie pożaru.

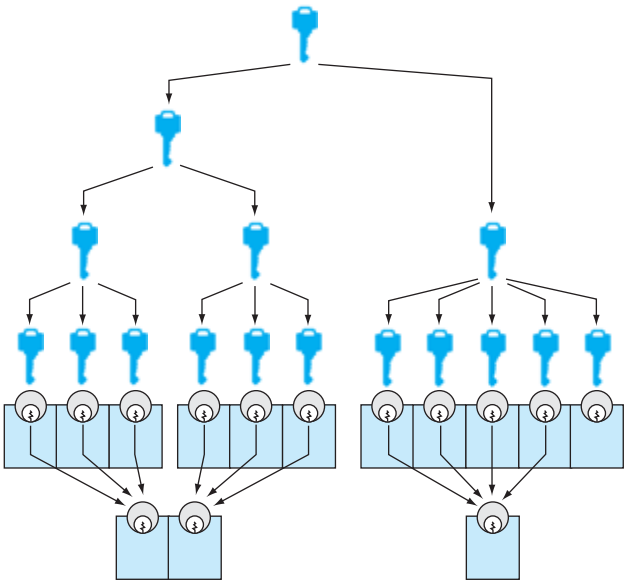
Minimalne wymagania dotyczące systemu

– opatentowany wzór klucza (zalecany, dopuszczalny jest klucz zastrzeżony) – gwarantuje właścicielowi systemu/firmy, że pracownicy nie będą w stanie dorobić sobie kopii kluczy bez wiedzy właściciela/administratora systemu;
– certyfikat klasy 6/2/C (właściwości zabezpieczeniowe) wg PN-EN1303:2007 i KT/402/IMP/2009, wydany przez Instytut Mechaniki Precyzyjnej lub Instytut Techniki Budowlanej;
– klasa trwałości 6 wg PN-EN1303:2007;
– oficjalny dokument z IMP lub ITB potwierdzający, że wkładki są zgodne z Polską Normą PN-78/B-94461-07, więc można je zastosować w układach centralnego otwierania;
– lokalny serwis zapewniany przez autoryzowanego partnera producenta.

Biurowce, fabryki, centra handlowe, hotele, urzędy, sądy, uczelnie itp. – system klucza generalnego

Zasada działania

Każdy z pracowników posługuje się jednym kluczem, którym otwiera swoje biuro i pomieszczenia wspólne (np. kuchnię, szatnię, toalety itp.). Kierownicy/managerowie otwierają pomieszczenia w działach, którymi kierują, służby techniczne – wszystkie



Rys. 2. System klucza generalnego

pomieszczenia techniczne, personel sprzątający – pomieszczenia, które regularnie sprząta itd., natomiast dyrektor administracyjny swoim jednym kluczem otwiera wszystkie pomieszczenia. Klucz generalny otwierający wszystkie pomieszczenia powinien być zdeponowany w bezpiecznym miejscu u ochrony (np. w kopercie bezpiecznej w sejfie lub depozytorze) –jako klucz przeciwpożarowy umożliwiający ewakuację osób i wartościowego sprzętu w razie pożaru czy innych kryzysowych sytuacji.

Zalecane jest zastosowanie depozytora kluczy dającego pełną kontrolę nad obiegiem kluczy systemowych w firmie (pobieranie klucza przy wejściu do siedziby firmy i zdanie go przed wyjściem).

Minimalne wymagania dotyczące systemu

– opatentowany wzór klucza – gwarantuje właścicielowi systemu/firmy, że pracownicy nie będą w stanie dorobić sobie kopii kluczy bez wiedzy właściciela/administratora systemu;
– certyfikat klasy 6/2/C (właściwości zabezpieczeniowe) wg PN-EN1303:2007 i KT/402/IMP/2009, wydany przez Instytut Mechaniki Precyzyjnej lub Instytut Techniki Budowlanej;
– klasa trwałości 6 wg PN-EN1303:2007;
– oficjalny dokument z IMP lub ITB potwierdzający, że wkładki są zgodne z Polską Normą PN-78/B-94461-07, więc można je zastosować w układach centralnego otwierania;
– lokalny serwis zapewniany przez autoryzowanego partnera producenta.

Profesjonalni użytkownicy końcowi (sektor energetyczny, paliwowy, gazowniczy, telekomunikacyjny, wojsko oraz banki)

Zasada działania (na przykładzie zakładu energetycznego)

Dyrektor działu eksploatacji sieci elektroenergetycznej posiada klucz, którym otwiera wszystkie punkty zasilania w firmie (GPZ, SN, NN). Pogotowie Energetyczne posługuje się kluczem, którym otwiera wszystkie punkty zasilania na obsługiwanym przez siebie obszarze. Pracownicy odczytujący stany liczników otwierają tylko skrzynki przyłączeniowe odbiorców (NN).

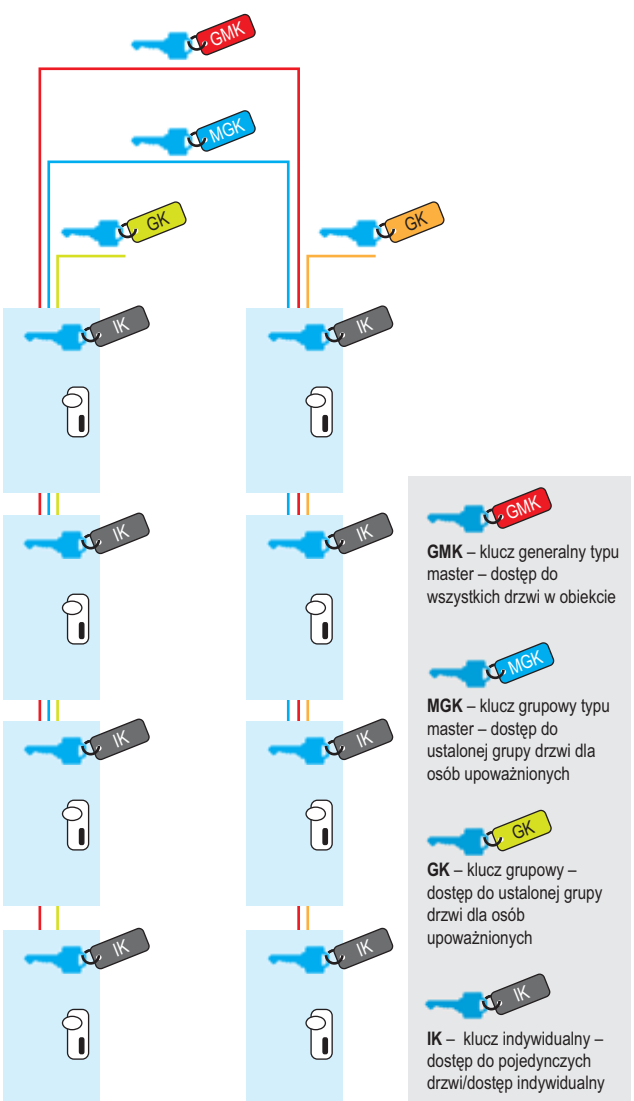
W przypadku zastosowania zamknięć (wkładek, kłódek) oraz kluczy elektromechanicznych do strategicznych pomieszczeń (np. GPZ) istnieje możliwość sczytywania informacji

o zdarzeniach zarówno z wkładek/kłódek (jaki klucz i kiedy je otwierał), jak i z kluczy (jakie zamknięcia i kiedy otwierał dany użytkownik/klucz), a także możliwość szybkiego zablokowania dostępu do pomieszczeń, jeśli na przykład pracownik nie oddał klucza bądź klucz został skradziony.

Zalecane jest zastosowanie depozytora kluczy dającego pełną kontrolę nad obiegiem kluczy systemowych w firmie (pobranie klucza przed rozpoczęciem zmiany i zdanie go po jej zakończeniu).

Minimalne wymagania, co do produktu

– odporność na pracę w trudnych warunkach środowiskowych (narażenie na korozję, zapiaszczenie, oddziaływanie niskich temperatur itp.) – w takich warunkach najlepiej radzą sobie mechanizmy dyskowe we wkładkach/kłódkach;
– opatentowany wzór klucza – gwarantuje właścicielowi systemu/firmy, że pracownicy nie będą w stanie dorobić sobie kopii kluczy bez wiedzy właściciela/administratora systemu;
– certyfikat klasy 6/2/C (właściwości zabezpieczeniowe) wg PN-EN1303:2007 i KT/402/IMP/2009, wydany przez Instytut Mechaniki Precyzyjnej lub Instytut Techniki Budowlanej;
– klasa trwałości 6 wg PN-EN1303:2007;
– klasa odporności na korozję C wg PN-EN1303:2007;



Rys. 3. Schemat systemu klucza generalnego – klucz generalny (master) + klucze grupowe (slave) + klucze indywidualne

– oficjalny dokument z IMP lub ITB potwierdzający, że wkładki są zgodne z Polską Normą PN-78/B-94461-07, więc można je zastosować w układach centralnego otwierania;
– zapewnienie producenta o swojej ugruntowanej pozycji na rynku (producent musi otrzymywać dostawy i zapewniać serwis przez okres co najmniej dziesięciu lat);
– pięcioletnia gwarancja na działanie produktów w każdych warunkach środowiskowych.

Wielu Polaków uważa, że dostateczną ochronę zapewnia system alarmowy. Nic bardziej mylnego. Powinniśmy stosować również odpowiednie, solidne zabezpieczenia mechaniczne, na przykład antywłamaniowe drzwi z wysokiej klasy wkładką bębenkową odporną na manipulacyjne metody otwierania (m.in. tzw. bumping), z szyldem chroniącym ją przed rozwierceniem, okna z okuciami antywłamaniowymi i z klamką na klucz (najlepiej z szybą klasy P4), które stawiają opór włamywaczowi i mogą zadecydować o tym, czy intruz dostanie się do środka, czy też pod presją czasu zrezygnuje z próby wejścia do czyjegoś domu. Pamiętajmy, że wybieramy zabezpieczenie domu, mieszkania czy firmy raz na długie lata. Jest to związane z wydatkiem, ale jednorazowym, a poczucie bezpieczeństwa jest bezcenne, dlatego wybierajmy rozwiązania renomowanych producentów, które spełniają określone w normach wymagania, zwracając szczególną uwagę na faktyczną ochronę klucza przez nieautoryzowanym dorobieniem.

W związku z tym, że mówimy o bezpieczeństwie, pojęciem, które nasuwa się automatycznie jest zaufanie. Zaufanie do firmy/osoby, która będzie Państwu rekomendowała, projektowała, dostarczała, montowała i serwisowała system klucza.

Warto sprawdzić, czy taka firma ma doświadczenie – jak długo działa na rynku i jakie ma referencje. Dzięki temu nawet po kilku latach będziemy mieli do kogo zwrócić się w sprawie wykonania kolejnych wkładek do systemu czy dorobienia kolejnych kluczy systemowych. Należy sprawdzić, czy firma ma oficjalną autoryzację producenta, którego produkty Państwu oferuje. Pracownik firmy, który projektuje system klucza generalnego powinien posiadać licencję II stopnia pracownika ochrony mienia wydaną przez Komendanta Wojewódzkiego Policji (zgodnie z ustawą o ochronie osób i mienia z 22.08.1997). Pamiętajmy, że system klucza generalnego jest elementem systemu bezpieczeństwa całego obiektu i jego zaprojektowanie wymaga wysokich kwalifikacji oraz pełnej poufności. Firma oferująca system klucza generalnego powinna mieć koncesję MSWiA (zgodnie z ustawą o ochronie osób i mienia z 22.08.1997). Taka koncesja jest bezwzględnie konieczna w przypadku obsługi obiektów objętych ochroną obowiązkową, których listę sporządza właściwy Wojewoda (zgodnie z przytoczoną powyżej ustawą o ochronie osób i mienia). W przypadku obsługi pozostałych obiektów taka koncesja nie jest obowiązkowa, ale warto skorzystać z oferty firmy, która ją posiada. Świadczy ona o najwyższym poziomie profesjonalizmu firmy oraz poufności i bezpieczeństwa danych związanych z zastosowanym u klienta systemem klucza generalnego. Najprostszym sposobem zweryfikowania wiarygodności firmy, która oferuje system klucza generalnego, jest wizyta na stronie producenta i sprawdzenie, czy dana firma jest autoryzowanym dystrybutorem.

Opracował
mgr inż. Mariusz Mikołajewski
Assa Abloy

Środki bezpieczeństwa fizycznego w ochronie informacji niejawnych (cz. 1)

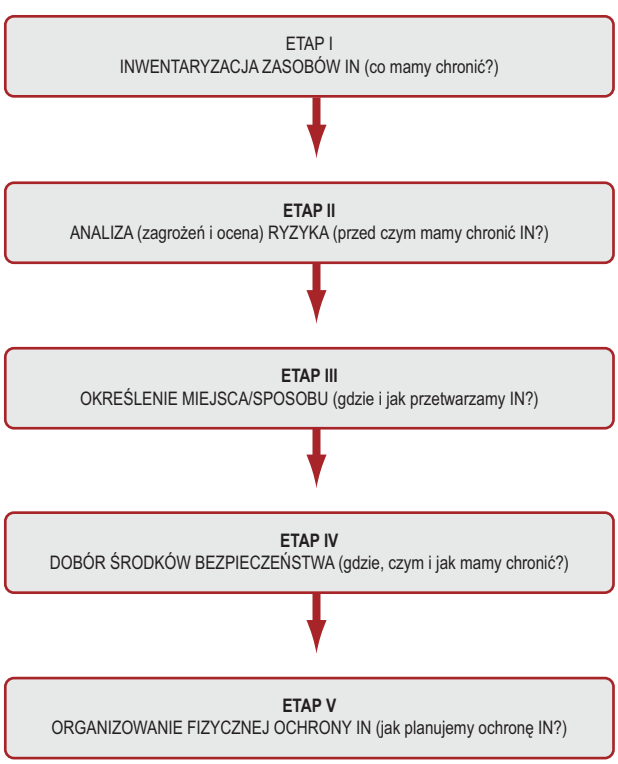
Artur Bogusz, Marek Blim

Główną kwestią do której chcemy się odnieść (w tej i kolejnych częściach cyklu), jest fizyczne zabezpieczanie informacji niejawnych i stosowne wymagania określone w rozporządzeniu Rady Ministrów z dnia 29 maja 2012 roku (publikacja z dn. 19 czerwca 2012 r – Dz. U. 2012r, poz. 683)

Omawiany dokument ma ujednolicić oraz uprościć procedury wyboru i stosowania środków bezpieczeństwa fizycznego w jednostkach organizacyjnych zobowiązanych do ochrony posiadanych informacji niejawnych zgodnie z opracowaną i załączoną metodyką oceny zarówno zagrożeń, jak i stanu posiadanych zabezpieczeń (określonych enumeratywnie wg kategorii i przypisanych im środków technicznych). Niestety nie wszystko jest zupełnie jasne. Spróbujmy zatem prześledzić dokładniej treść tego dokumentu oraz jego załączników. Całość cyklu obejmie następujące zagadnienia:

1) algorytmizacja zadania ochrony (czyli to, co musimy zrobić);
2) określenie zagrożeń (czyli to, co wpływa na ryzyko ujawnienia lub utraty informacji);
3) atrybuty informacji a aspekty ochrony (czyli jakie mamy środki ochrony);
4) dostęp do informacji, nośników systemów (czyli jakie są kryteria strefowania);
5) tabelaryzacja rozwiązań ochronnych (czyli obliczanie wpływu użytych środków w danej kategorii ochronnej);
6) plan ochrony (czyli kwintesencja naszych działań);
7) podsumowanie (czy i kiedy sami wprowadzamy zmiany).

Zainteresowanych czytelników zapraszamy do dyskusji i wymiany poglądów na forum *Zabezpieczeń*. Praktycy mogą podzielić się własnymi doświadczeniami, szkoleniowcy – dodać merytoryczne uwagi, a decydenci – opisać własne rozstrzygnięcia kwestii organizacyjnych. Wszyscy możemy uczestniczyć w podwyższaniu poziomu wiedzy i kultury ochrony informacji.



Rys. 1. Uproszczony algorytm postępowania w ochronie fizycznej zasobów informacji niejawnej (IN)

Algorytmizacja zadań ochrony

Proponujemy, aby całość nakazów i zaleceń ujętych w rozporządzeniu analizować etapami, według uproszczonego algorytmu przedstawionego na rysunku 1, co pozwoli na lepsze zrozumienie poszczególnych kwestii wynikających z treści rozporządzenia. Do niektórych z nich podejdziemy modelowo, w sposób procesowy – wyodrębniony na bazie dostępnych metod i norm. Zainteresowanych obszerniejszym uzasadnieniem takiego sposobu postępowania odsyłamy do metod systemowych[1]. Wierzymy, że użyteczność tego podejścia i uzyskanej grupy rozwiązań będzie miała dostateczne potwierdzenie w dalszej części naszych wywodów.

Rozporządzenie jest ustawowym aktem nakazowym i pozostawia nam do wyboru jedynie czas realizacji opisanych w nim zadań, określając jednoznacznie (patrz §10[2]) trzyletni termin na wykonanie wszystkich prac (tzn. do dnia 4 lipca 2015 roku).

Należy pamiętać, że mówimy tutaj o modelowym postępowaniu, czyli że wielkość obszaru objętego działaniami na danym etapie postępowania zależy od decydenta – kierownika jednostki organizacyjnej. Określa on nie tylko to, co, gdzie i kiedy robimy, ale także to, w jaki sposób oceniamy wyniki tej pracy – na podstawie wytycznych i wymagań zawartych w przedmiotowym rozporządzeniu.

Pamiętajmy, że zawsze możemy zrobić więcej, ale nie wolno nam zrobić mniej niż wymaga ustawodawca.[3]

Chroniony zasób informacji niejawnych

Zanim przystąpimy do czynności inwentaryzacyjnych, zastanówmy się, co jest zasobem informacji niejawnych według rozporządzenia Rady Ministrów, zwłaszcza po przeanalizowaniu zapisów ustawy o ochronie informacji niejawnych[4] dotyczących informacji, danych, dokumentów i materiałów niejawnych oraz zasad ich przetwarzania.

1) Góralski A. „Zadanie, metoda, rozwiązanie. Techniki twórczego myślenia". zbiór II, wyd. WNT, Warszawa 1979.

2) Rozporządzenie Rady Ministrów, poz. 683/2012 „§10.1. W terminie 3 lat od dnia wejścia w życie rozporządzenia określa się poziom zagrożeń, opracowuje dokumenty, o których mowa w § 9, i dostosowuje się kombinację środków bezpieczeństwa fizycznego oraz organizację stref ochronnych do wymagań określonych w rozporządzeniu."

3) §9, ust. 2, s 5 rozporządzenia Rady Ministrów, poz. 683/2012.

4) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnej (Dz. U. z 2010 r., nr 182 poz.1228)

Wskazanie w ustawie konieczności stosowania w ochronie samych informacji niejawnych środków bezpieczeństwa fizycznego[5], wraz z delegacją wykonawczą[6] wcale jednoznacznie nie rozstrzyga pojawiających się wątpliwości, co do ochrony ich przetwarzania (patrz: §8 ust.5 rozporządzenia).

Możemy i powinniśmy traktować jako zasób wszelkie zapisy informacji niejawnych niezależne od ich nośnika, wytworzone w danej jednostce organizacyjnej lub otrzymane z zewnątrz (do wiadomości, wykorzystania, przetworzenia lub powierzone do zapoznania i okresowego przechowywania). Mogą to być wydruki „hard copy", mapy, fotografie, fotokopie, dokumenty zbroszurowane i edytowane, nośniki OEM[7], a ich ilość, klauzule oraz sposób ich udostępniania/przetwarzania (liczba osób, miejsce), wpływają znacząco na dalsze postępowanie z nimi w trybie nakazanym w rozporządzeniu.

Atrybuty chronionych informacji

Jako podstawowe atrybuty informacji niejawnych wymienione są zarówno w ustawie o ochronie informacji niejawnych, jak i w rozporządzeniu (patrz §2) trzy charakterystyczne właściwości informacji – poufność, integralność oraz dostępność. Przekłada się to na sposób dokonywania inwentaryzacji posiadanego zasobu z racji różnych klauzul ochronnych (poufność), ograniczonego ujawniania użytkownikom – zasada „wiedzy potrzebnej" (dostępność), oraz możliwości formalnych w zakresie wykonanych/wykonywanych wypisów i wyciągów z dokumentów (dostępność), szczególnie w aspekcie możliwości zaistnienia incydentów bezpieczeństwa.

Aspekty ochrony zasobu informacyjnego

Sama inwentaryzacja informacji niejawnych wymaga już na wstępie uwzględnienia kilku istotnych kwestii jako zadań/problemów do późniejszego rozpatrzenia. Są to przede wszystkim:

- wyodrębnione przez ustawodawcę, w załącznikach do rozporządzenia, kategorie ochrony i różne środki (organizacyjne oraz materiałowo-techniczne) służące do ich zapewnienia,
- pozostawione do indywidualnych decyzji kierownika jednostki organizacyjnej obszary i sposoby działania w zakresie zapewnienia ochrony fizycznej na wymaganym przez ustawodawcę poziomie,
- istniejące informacje i dokumenty niejawne przychodzące z zewnątrz o narzuconym z góry (wymóg sojuszniczy/układowy) sposobie zapewnienia ochrony (np. informacja niejawna z klauzulą NCA[8]).

Podsumowanie I etapu

Profesor Tadeusz Kotarbiński stwierdził, że można robić wiele, lecz nie da się zarządzać niewiedzą. Jakże często posiadana przez nas wiedza jest niekompletna – i to tylko w wyniku niedostatecznego starania się o jej pozyskanie, czy uporządkowanie tej już posiadanej.

W swojej dotychczasowej praktyce zawodowej i audytorskiej napotkaliśmy mnóstwo negatywnych przykładów z tego zakresu. Mamy w związku z tym kilka sugestii:

- należy dostrzegać szczególne znaczenie uporządkowania wiedzy (w tym ukrytej, nie skodyfikowanej) dotyczącej określania uwarunkowań oraz zabezpieczeń ochrony informacji niejawnych związanych z pełnieniem funkcji przez osoby fizyczne,
- należy zauważać i minimalizować tendencję „spychania" obowiązków związanych z ochroną informacji niejawnych na pełnomocnika do spraw ochrony informacji niejawnych, gdyż rzeczywiste bezpieczeństwo zapewniają wszyscy pracownicy – świadomi swoich obowiązków w tym zakresie,
- wskazane jest cykliczne przypominanie użytkownikom informacji niejawnych, że nieznajomość przepisów nie zwalnia od odpowiedzialności za powierzony zasób informacji niejawnych (między innymi za zaniechanie działań, zaniedbania organizacyjne i błędy w inwentaryzacji).

Artur Bogusz
Marek Blim

Bibliografia

1. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, wyd. WNT, Warszawa 2006.
2. Cabała P., *Wprowadzenie do prakseologii. Przegląd zasad skutecznego działania*, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków 2007.
3. Ustawa o ochronie informacji niejawnych. Dz. U. z 2010 r, nr 182, poz. 1228,.
4. Rozporządzenie RM w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych. Dz. U. z dnia 19 czerwca 2012 r, poz. 683.
5. Góralski A., *Być nowatorem*, PWN, Warszawa 1990.
6. Góralski A., *Zadanie, metoda, rozwiązanie. Techniki twórczego myślenia*, wyd. WNT, Warszawa 1977-1984 (pięć zbiorów)
7. *Procedury ochrony informacji niejawnych w praktyce*, praca zbiorowa, wyd. FORUM, Poznań 2011.

5) Ibidem: Art. 1 ust.1. pkt 8.

6) Ibidem: Art. 47 ust. 1.

7) Do nośników z zapisem optyczno-elektroniczno-magnetycznym zaliczamy płyty CD, pendrive, pamięci flash, taśmy magnetyczne steamerów, zewnętrzne przenośne dyski z danymi (niezależnie od typu) itp.

8) NCA (NATO Confidential Atomal) – poufna informacja NATO, która może dotyczyć np. przewozu promieniotwórczych odpadów z elektrowni jądrowej, które mogą być wykorzystane jako składnik „brudnej bomby" budowanej przez terrorystów.

Ty i Twoi klienci możecie spać bezpieczniej

z systemem PowerMaxExpress!

Wysoce stabilny i **niezawodny**
bezprzewodowy system alarmowy

Oszczędzasz czas i **pieniądze**
dzięki szybkiej i bezproblemowej instalacji!

Visonic
A Tyco International Company

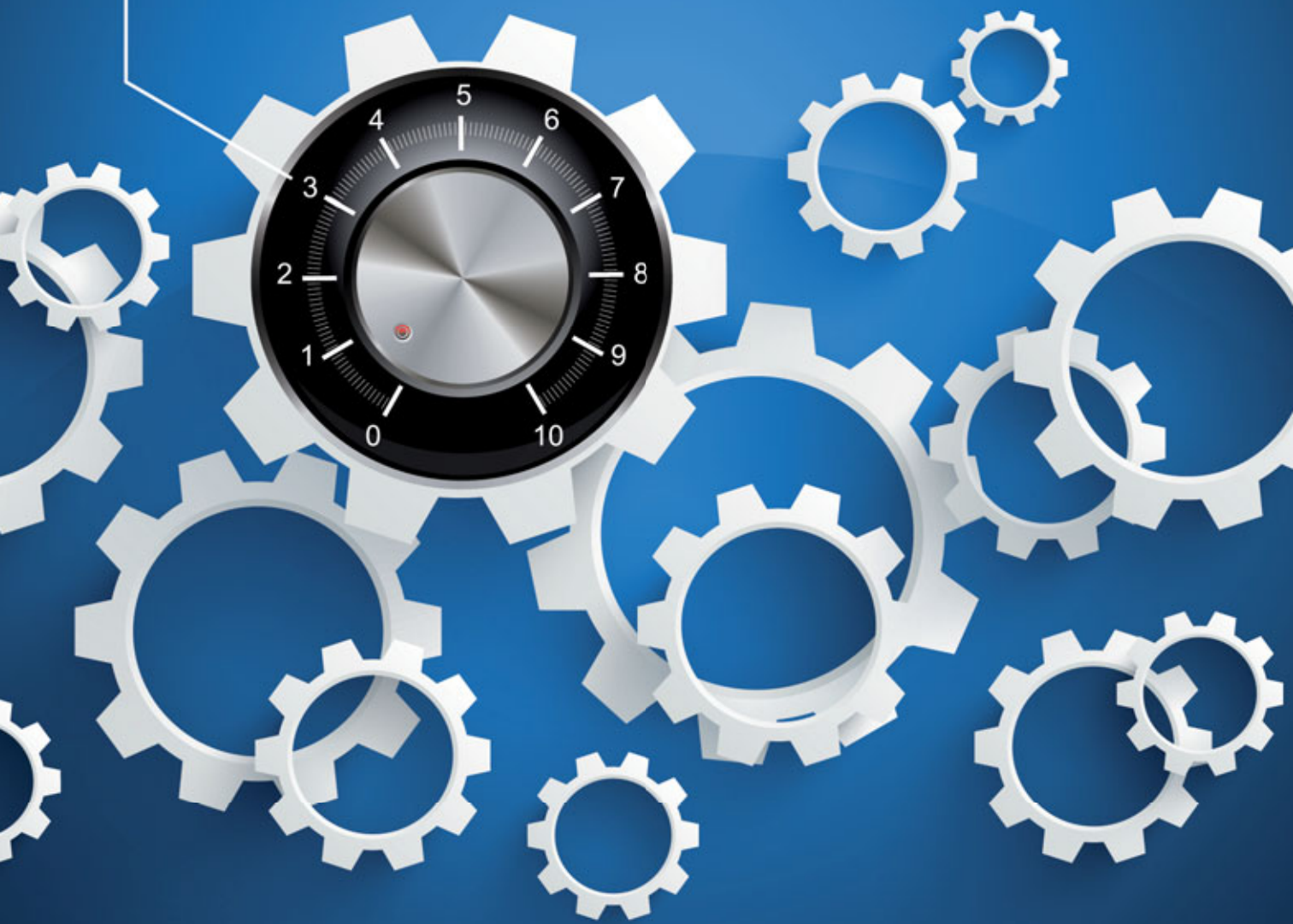
Wyłączny dystrybutor produktów Visonic w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Stosowanie środków bezpieczeństwa fizycznego w ochronie informacji niejawnych

Marek Protekta

Nareszcie mamy rozporządzenie w sprawie środków bezpieczeństwa stosowanych do zabezpieczania informacji niejawnych. Rozporządzenie jest z dnia 29 maja 2012 r. i weszło w życie po 14 dniach od daty ogłoszenia czyli od 19 czerwca 2012 r. pod pozycją 683 w Dzienniku Ustaw RP



Już w 1999 roku, w związku z tworzeniem ustawy o ochronie informacji niejawnych, pojawiła się koncepcja stworzenia dokumentu określającego środki bezpieczeństwa. Niestety pośpiech i potrzeba szybkiego wydania ustawy (presja czasu wynikająca z trwającego procesu akcesji do NATO) spowodowały, że odłożono to na później. Przy nowelizacji treści ustawy w 2005 r. chyba zapomniano o tym pomocniczym, a jakże istotnym dokumencie i znowu niestety nie powstał, mimo potwierdzonej wcześniej potrzeby uregulowania tych spraw. Prace nad nim rozpoczęto przy okazji tworzenia nowej (co do zakresu) ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 r. (Dz. U. 182, poz. 1228) i „oto jest".

Nareszcie jest „waga", którą możemy „zważyć" środki bezpieczeństwa, które już zostały zastosowane w celu ochrony naszych informacji niejawnych. Dzięki rozporządzeniu i załączonej do niego metodyce możemy sprawdzić, czy nasza koncepcja konfiguracji środków bezpieczeństwa spełni oczekiwania ustawodawcy i zabezpieczy posiadane przez nas informacje niejawne przed ich nieuprawnionym ujawnieniem lub utratą. Nie bez znaczenia są koszty, które musimy ponieść, organizując fizyczną ochronę informacji niejawnych.

Należy zwrócić uwagę na to, że ustawodawca nałożył na kierownika jednostki organizacyjnej, w której przetwarzane są informacje niejawne, odpowiedzialność za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony (art. 14 ust. 1 ustawy o ochronie informacji niejawnych), a co za tym idzie również odpowiedzialność za prawidłowe określenie „poziomu zagrożeń". Dlatego zgodnie z rozporządzeniem, bez względu na to, czy już mamy system ochrony informacji niejawnych, czy będziemy go dopiero tworzyć, musimy rozpocząć od określenia zagrożeń.

Jednostka organizacyjna posiadająca już system ochrony ma trzy lata od dnia wejścia w życie rozporządzenia na określenie poziomu zagrożeń (§ 10.1 rozporządzenia). W celu określenia tego poziomu przeprowadza się analizę, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych. Podstawowe kryteria i sposób określania ryzyka nieuprawnionego ujawnienia lub utraty informacji niejawnych są zawarte w załączniku nr 1 do rozporządzenia. Z mojego doświadczenia wynika, że nie należy określać poziomu zagrożeń samodzielnie – to zbyt duża odpowiedzialność. Kierownik jednostki organizacyjnej powinien powołać w tym celu zespół projektowo-zadaniowy. W jego skład powinni wejść obecni lub przyszli pracownicy pionu ochrony informacji niejawnych, administrator systemu przeznaczonego do przetwarzania informacji niejawnych lub kandydat (kandydaci) na to stanowisko, przedstawiciel komórki zajmującej się ochroną fizyczną obiektu oraz osoba odpowiedzialna za administrowanie obiektem. Chociaż jedna z osób wchodzących w skład zespołu, najlepiej pełnomocnik ds. ochrony informacji niejawnych, który prawdopodobnie zostanie wyznaczony na przewodniczącego zespołu, powinna posiadać odpowiednią wiedzę na temat posługiwania się *Tabelą oceny istotności czynników zagrożeń* (załącznik nr 1 do rozporządzenia).

Wypełniając tabelę (z zał. nr 1), należy brać pod uwagę wszystkie czynniki mające wpływ na zagrożenie informacji niejawnych. Trzeba jednak umieć wskazać najistotniejsze z nich. Jeżeli mamy wątpliwości, czy wybrany czynnik jest mniej czy bardziej istotny, lepiej założyć, że jest bardziej istotny. Należy postąpić tak samo, jeżeli wynik z tabeli jest na granicy poziomu niższego i wyższego. Przyjmujemy poziom wyższy, podając w uzasadnieniu powód takiego postępowania. Zwróćmy uwagę na to, że przy klauzuli „ściśle tajne" ustawodawca sam określił stałą wartość oceny (osiem punktów) i dotyczy to również nowo tworzonej jednostki organizacyjnej przygotowującej się do przetwarzania informacji niejawnych o tej klauzuli.

Istotność czynnika „liczba materiałów niejawnych" wynika z klauzuli i ilości materiałów niejawnych o najwyższej klauzuli, którymi jednostka organizacyjna faktycznie dysponuje, tj. ilości materiałów przechowywanych w niej, a niezarejestrowanych w dzienniku ewidencji materiałów niejawnych. Możemy mieć na przykład 2000 dokumentów niejawnych oznaczonych klauzulą

„tajne" zarejestrowanych w ciągu ostatniego roku, ale 998 z nich, tj. kolejne 998 numerów w dzienniku ewidencji, bowiem sporządzono w pojedynczych egzemplarzach i wysłano do adresatów wraz z egzemplarzem nr 1 pisma korespondencyjnego (przewodniego). Na każdym z pism korespondencyjnych znajduje się „Po odłączeniu załączników – JAWNE", co oznacza, że ich egzemplarze pozostające w naszej jednostce organizacyjnej bez załączników są jawne i nie podlegają takiej ochronie jak dokumenty niejawne. Dwa dokumenty wykonano w czterech egzemplarzach (po dwa egzemplarze każdego z nich) – po jednym egzemplarzu wysłanym do adresatów i po jednym dla kancelarii tajnej naszej jednostki organizacyjnej. Oznacza to, że faktycznie mamy w kancelarii tajnej tylko dwa dokumenty niejawne, tj. 0, 1% wszystkich zarejestrowanych dokumentów. Jeżeli jest to tendencja, która utrzymuje się od kilku lat, i prognozujemy, że w następnym roku będzie podobna, należy rozważyć określenie zagrożenia jako mało istotnego (o ważności 1 pkt).

Określając „postać informacji niejawnych", należy brać pod uwagę ogólną liczbę przetwarzanych informacji niejawnych, stosując zasadę, że im więcej informacji jest przetwarzanych w systemie teleinformatycznym (w stosunku do ogólnej liczby materiałów), tym czynnik jest bardziej istotny (głównie ze względu na rodzaj nośnika).

Oceniając „liczbę osób", należy uwzględnić pracowników jednostki organizacyjnej mających lub mogących mieć dostęp do informacji niejawnych, a także uzasadnioną potrzebę dostępu do tych informacji. Im więcej osób (w stosunku do liczby zatrudnionych), tym czynnik jest bardziej istotny.

Czynnik „lokalizacji" zależy między innymi od tego, czy budynek jest w zabudowie zwartej (ściany budynku przylegają do innego budynku). Na wzrost istotności czynnika ma w tym przypadku wpływ tzw. „niebezpieczne sąsiedztwo", jakim może być obiekt przedstawicielstwa korporacji ponadnarodowej, podmiotu zagranicznego, hotel, obiekt sportowy lub hala widowiskowa, ogólnodostępny parking lub garaż, zakład przemysłowy i instalacje stanowiące zagrożenie dla życia i zdrowia.

„Dostęp osób do budynku" jest czynnikiem istotnym albo nieistotnym w zależności od tego, czy osoby, które nie są pracownikami jednostki organizacyjnej, mogą swobodnie poruszać się po budynku. Problem dotyczy najczęściej obiektów użyteczności publicznej.

Wskazując „inne czynniki" mające wpływ na zagrożenie, powinno się uwzględnić specyfikę jednostki organizacyjnej. Tymi czynnikami mogą być np. zagrożenie działaniami obcych służb specjalnych (np. jednostka organizacyjna produkuje uzbrojenie lub części do niego i posiada niejawną dokumentację technologii produkcji), zagrożenie sabotażem (np. zagrożenie uszkodzeniem komputerowego systemu sterowania przesyłem energii elektrycznej w elektrowni na skutek uzyskania przez kogoś nieuprawnionego dostępu do dokumentacji niejawnej), zagrożenie zamachem terrorystycznym lub inną działalnością przestępczą, pożarem, działaniem sił przyrody (np. zagrożenie powodzią) lub szkodami górniczymi. Jeśli kierownik jednostki organizacyjnej dostrzega inne czynniki mające wpływ na zagrożenie ujawnieniem lub utratą informacji niejawnych, powinien je określić i uzasadnić swoje stanowisko (rubryka „uzasadnienie"). W przypadku występowania więcej niż jednego „innego czynnika" należy oszacować je łącznie i ocenić ich wpływ na zagrożenie. Jeżeli jeden z czynników tej grupy uznaliśmy za „bardzo istotny", a inne za mniej istotne, należy ocenić je razem tak jak najistotniejszy z nich, czyli – w tym przypadku – jako „bardzo istotne". Jeżeli kierownik jednostki organizacyjnej uzna, że w jego jednostce czynniki wymienione w tabeli są nieistotne lub ich występowanie jest mało realne, np. zagrożenie ze strony obcych służb specjalnych, „inne czynniki" powinny zostać ocenione jako „mało istotne".

W przypadku nowo organizowanego systemu ochrony informacji niejawnych należy przyjąć wartości szacunkowe dla czynników: „klauzula tajności przetwarzanych informacji niejawnych", „liczba materiałów niejawnych", „postać informacji niejawnych" i „liczba osób".

Dokonawszy „oceny istotności czynnika", po podsumowaniu punktów wskazanych w pozycjach 1-7 tabeli zał. nr.1, uzyskujemy wynik określający poziom zagrożenia – według *Tabeli do określania poziomu zagrożeń* (do 16 punktów – poziom niski, od 17 do 32 punktów – poziom średni, powyżej 32 punktów – poziom wysoki). Po jego określeniu można przystąpić do określenia adekwatnych środków bezpieczeństwa fizycznego.

Środki bezpieczeństwa stosuje się w celu zapewnienie poufności, integralności i dostępności informacji niejawnych (dostępność informacji niejawnej – informacja niejawna jest możliwa do wykorzystania na żądanie podmiotu uprawnionego w określonym czasie, integralność informacji niejawnej – informacja niejawna nie została zmodyfikowana w sposób nieuprawniony, poufność informacji niejawnej – informacja niejawna nie została ujawniona podmiotom do tego nieuprawnionym).

Cel osiąga się przez:

– zapewnienie właściwego przetwarzania informacji niejawnych,
– umożliwienie zróżnicowania dostępu pracowników do informacji niejawnych zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji niejawnych (zasada „wiedzy potrzebnej"),
– wykrywanie i udaremnianie działań nieuprawnionych,
– uniemożliwienie lub opóźnienie wtargnięcia osób nieuprawnionych (w sposób niezauważony lub z użyciem siły) do pomieszczenia lub na obszar, w którym przetwarzane są informacje niejawne.

Do środków bezpieczeństwa fizycznego należą rozwiązania organizacyjne, wyposażenie i urządzenia służące do ochrony informacji niejawnych oraz elektroniczne systemy pomocnicze wspomagające ochronę informacji niejawnych. W zależności od uzyskanego wyniku oceny poziomu zagrożeń stosuje się odpowiednią kombinację środków bezpieczeństwa fizycznego. Środki te są następujące:

1. Personel bezpieczeństwa – osoby przeszkolone, nadzorowane, w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, m.in. kontrolujące dostęp do miejsc, w których przetwarzane są informacje niejawne, nadzorujące system dozoru wizyjnego, a także reagujące na alarmy lub sygnały awaryjne.

Takim personelem bezpieczeństwa są pracownicy kancelarii tajnej i pracownicy firmy posiadający poświadczenia bezpieczeństwa, w tym ci, którzy ochraniają obiekt, lub pracownicy firmy zewnętrznej, która uzyskała świadectwo bezpieczeństwa przemysłowego, również posiadający poświadczenia bezpieczeństwa.

2. Bariery fizyczne – środki chroniące granice miejsca, w którym są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna.

3. Szafy i zamki – stosowane do przechowywania dokumentów z informacjami niejawnymi lub zabezpieczające te dokumenty przed nieuprawnionym dostępem.

Szafy i zamki muszą posiadać certyfikaty potwierdzające ich klasę, a szafa dodatkowo tabliczkę znamionową z nazwą producenta, typem wyrobu, numerem wyrobu, klasą wyrobu i numerem certyfikatu.

4. System kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania wyłącznie osobom posiadającym odpowiednie uprawnienia dostępu do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

System kontroli dostępu wchodzący w skład elektronicznego sytemu pomocniczego, jakim jest SSWiN, jest rozwiązaniem prostym i niedrogim. Wykorzystanie go do rejestrowania wejść osób uprawnionych do strefy ochronnej II jest bardzo korzystne. Pozostałe osoby też trzeba rejestrować, np. w dzienniku osób przebywających w strefie ochronnej II. Odnotowywanie „na papierze" wszystkich wejść do strefy ochronnej II jest gorszym rozwiązaniem.

5. System sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach – zastępujący lub wspierający personel bezpieczeństwa.

Elektroniczny system pomocniczy wspierający ochronę informacji niejawnych powinien posiadać wydane przez dostawcę poświadczenie zgodności z wymogami określonymi w normie PN-EN 50131-1 wymienionej w rozporządzeniu (z uwzględnieniem przepisów dotyczących oceny zgodności).

6. System dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów zagrażających bezpieczeństwu i sygnałów alarmowych przez personel bezpieczeństwa.

7. System kontroli osób i przedmiotów – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na proszeniu o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych (w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego „wynoszenia" informacji niejawnych z miejsc, w których są przechowywane).

Jeżeli z analizy poziomu i oceny punktowej zagrożenia wynika taka potrzeba, można zastosować również inne środki bezpieczeństwa, które zapewnią poufność, integralność i dostępność informacji niejawnych.

W przypadku istnienia zagrożenia podglądem/podejrzeniem informacji niejawnych (także przypadkowym), zarówno w świetle dziennym i przy sztucznym oświetleniu, należy podjąć działania eliminujące to zagrożenie.

Ustawodawca zmienił obowiązujące dotychczas nazwy stref.

1. Strefa ochronna I – obejmuje miejsce (pomieszczenie lub obszar), w którym informacje niejawne o klauzuli „poufne" lub wyższej są przetwarzane w taki sposób, że dostęp do tego

miejsca umożliwia uzyskanie bezpośredniego dostępu do tych informacji, miejsce to spełnia następujące wymagania:
- w planie ochrony wyraźnie wskazana jest najwyższa klauzula tajności przetwarzanych informacji niejawnych;
- granice są wyraźnie określone i zabezpieczone;
- zastosowany jest system kontroli dostępu, który zezwala na wstęp osób, które są uprawnione do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy, pełnienia służby lub wykonywania czynności zleconych;
- wstęp jest możliwy wyłącznie ze strefy ochronnej.

2. Strefa ochronna II (poprzednio – strefa bezpieczeństwa) – obejmuje miejsce (pomieszczenie lub obszar), w którym informacje niejawne o klauzuli „poufne" lub wyższej są przetwarzane w taki sposób, że dostęp do tego miejsca nie umożliwia uzyskania bezpośredniego dostępu do tych informacji, a miejsce to spełnia następujące wymagania:
- granice są wyraźnie określone i zabezpieczone;
- zastosowany jest system kontroli dostępu, który zezwala na wstęp osób, które są uprawnione do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy, pełnienia służby lub wykonywania czynności zleconych;
- w przypadku konieczności wstępu osób innych niż te, o których mowa w poprzednim podpunkcie, zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne;
- wstęp jest możliwy wyłącznie ze strefy ochronnej.

3. Strefa ochronna III (poprzednio – strefa administracyjna) – obejmuje miejsce (pomieszczenie lub obszar) wymagające wyraźnego określenia granic, w obrębie którego możliwe jest kontrolowanie osób i pojazdów.

Proces doboru środków bezpieczeństwa fizycznego powinien zapewnić elastyczność ich stosowania w zależności od określonego wcześniej (punktowo) poziomu występujących zagrożeń. W § 4–8 rozporządzenia przedstawione są podstawowe wymagania dotyczące doboru tych środków.

Pierwszym krokiem jest odczytanie z tabeli *Podstawowe wymagania dotyczące bezpieczeństwa fizycznego* minimalnej liczby punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiednich kombinacji środków bezpieczeństwa fizycznego. Wymagana suma punktów zależy od najwyższej klauzuli tajności informacji niejawnych przetwarzanych w danej lokalizacji oraz sumarycznego poziomu zagrożeń określonego wcześniej. Należy przestrzegać wskazówek ustawodawcy dotyczących sumowania lub wymnażania – w każdej ocenianej kategorii – poszczególnych punktowych wartości przypisanych do użytych środków bezpieczeństwa.

Drugim krokiem jest odczytanie z tej samej tabeli minimalnej liczby punktów odpowiadającej – w każdej z grup obejmujących kategorie – wymaganemu i nakazanemu przez ustawodawcę poziomowi zabezpieczenia fizycznego.

Trzecim krokiem jest dokonanie wyboru określonych środków bezpieczeństwa fizycznego, przy którym należy posługiwać się tabelą *Klasyfikacja środków bezpieczeństwa fizycznego*. W tej tabeli należy odczytać liczbę punktów odpowiadającą wybranemu środkowi bezpieczeństwa i wpisać ją w odpowiednie miejsce tabeli *Punktacja zastosowanych środków bezpieczeństwa fizycznego*. Niezastosowanie danego środka jest jednoznaczne z przyznaniem mu liczby punktów „0". Przy dokonywaniu wyboru konieczne jest również uwzględnienie określonych w rozporządzeniu wartości „obowiązkowych" z tabeli *Podstawowe wymagania dotyczące bezpieczeństwa fizycznego*.

Np. przy klauzuli:
- „ściśle tajne":
  - kategorie K1 (szafy)+K2 (pomieszczenia)+K3 (budynki) – tylko jedna wartość może być równa 0 (zero),
  - kategorie K4 (kontrola dostępu)+K5 (personel bezpieczeństwa i systemy sygnalizacji włamania) – żadna z wartości nie może być mniejsza od 2;
- „tajne" kategorie K4 (kontrola dostępu)+K5 (personel bezpieczeństwa i systemy sygnalizacji włamania) – żadna z wartości nie może być równa 0 (zero).

Dobór adekwatnych środków bezpieczeństwa fizycznego w konkretnym przypadku musi zapewnić uzyskanie zarówno minimalnej sumy punktów wymaganej do osiągnięcia założonego poziomu ochrony informacji niejawnych (w zależności od najwyższej klauzuli tajności informacji przetwarzanych w danej lokalizacji oraz poziomu zagrożeń), jak również minimalnej liczby punktów odpowiadających każdej z grup kategorii środków bezpieczeństwa fizycznego (oznaczonych w tabeli *Podstawowe wymagania dotyczące bezpieczeństwa fizycznego* jako „obowiązkowe").

W przypadku, gdy liczba punktów uzyskanych po zastosowaniu środka bezpieczeństwa z kategorii „obowiązkowe" jest mniejsza od minimalnej liczby punktów wymaganych do osiągnięcia założonego poziomu ochrony, należy zastosować środki z kategorii oznaczonych „dodatkowe". W przypadku klauzuli „poufne" lub wyższej są to środki z kategorii K6 „Granice", do których należą:
- K6S1 – ogrodzenie,
- K6S2 – kontrola w punktach dostępu,
- K6S3 – system kontroli osób i przedmiotów przy wejściu/wyjściu,
- K6S4 – system wykrywania naruszenia ogrodzenia,
- K6S5 – oświetlenie chronionego obszaru,
- K6S6 – system dozoru wizyjnego granic.

Podsumowując, można powiedzieć, że proces wdrażania środków bezpieczeństwa fizycznego przebiega dwuetapowo. Na pierwszym etapie trzeba określić punktowo poziom zagrożenia, a na drugim – dobrać odpowiednie środki bezpieczeństwa w określonych kategoriach. Taki sposób postępowania muszą przyjąć firmy, które chcą prawidłowo zbudować system ochrony informacji niejawnych, i firmy już posiadające taki system ochrony, które chcą sprawdzić, czy zastosowały wystarczające środki bezpieczeństwa.

Do samego rozporządzenia nie mam uwag, natomiast mam pewne uwagi dotyczące klasyfikacji środków bezpieczeństwa fizycznego. Zmiana oznaczeń klasy odporności na S1 i S2 jest tylko dostosowaniem do nowszych norm. Niektóre sformułowania, np. „zapewnia wysoką odporność na działanie osoby nieuprawnionej", budzą moje wątpliwości. Ogrodzenie sprawi większości z firm mały kłopot. Ile firm posiada ogrodzenie o wysokości 250 cm i wolną przestrzeń między budynkami a ogrodzeniem o szerokości 25 m? O pozostałych wymaganych elementach zabezpieczających ogrodzenie nie wspomnę.

Życie zweryfikuje zapisy tego rozporządzenia. Mam nadzieję, że rozporządzenie pomoże wszystkim wybrać i zastosować odpowiednie środki bezpieczeństwa fizycznego.

Marek Protekta
Pełnomocnik ds. ochrony informacji niejawnych w firmie Siemens
Konsultant JDS CONSULTING

SAMSUNG

LiteNet

Promocja kamer LiteNet HD

SSN Security Solution Network

Szczegóły w sieci dystrybucji **www.ssn.net.pl**

ALPOL SECURITY SYSTEMS

ProfiCCTV

Cyfrowy algorytm detekcji CORE w nowych czujkach OPTEX

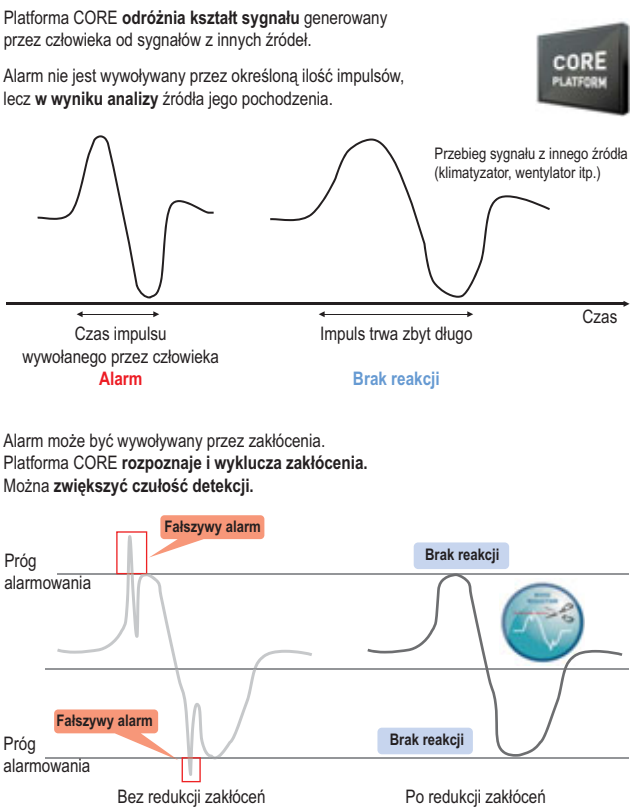
Jacek Wójcik

Wiosną 2012 roku OPTEX zaprezentował nowe wewnętrzne czujki ruchu RX CORE. Są one następcą, cieszącej się uznaniem instalatorów, serii czujek RX-40. Czujki wyposażono w zmienioną obudowę wykonaną z odpornego na przebarwienia polistyrenu, obrotowy uchwyt ścienno-sufitowy i bezgłośnie pracujący przekaźnik. Zastosowano też zupełnie nowy algorytm detekcji CORE. Czujka RXC-ST jest pierwszym modelem z nowej generacji czujek OPTEX wykorzystującym nowoczesną technikę przetwarzania sygnału przez mikroprocesor na podstawie cyfrowej analizy źródła jego pochodzenia. Firma zapowiada kolejne modele czujek wewnętrznych wykorzystujące technologię CORE: RXC-DT – czujkę dualną z nowym, precyzyjnym, odpornym na czynniki środowiskowe modułem mikrofalowym – oraz serię czujek CDX – czujki spełniające wymagania dla stopnia 3. normy EN50131 (powierzchniowa czujka PIR i czujka dualna oraz kurtyna PIR 24×2 m), przeznaczone do zastosowań komercyjnych

Klasyczne urządzenia wykrywające ruch dzięki technologii podczerwieni pasywnej wykorzystują metodę zliczania impulsów generowanych przez zmiany natężenia promieniowania podczerwonego. Pojawienie się obiektu, którego temperatura różni się od temperatury tła, na określonym obszarze podzielonym na pola detekcji powoduje zmianę napięcia w pyroelemencie. Przekroczenie przez napięcie wartości granicznej jest rejestrowane jako impuls. Czujka wysyła sygnał alarmowy po zarejestrowaniu ustalonej liczby impulsów. W konstrukcji czujki należy uwzględniać zdolność do rejestracji różnicy temperatury, która w połączeniu z odpowiednim elementem skupiającym (soczewką Fresnela lub lustrem skupiającym) decyduje o końcowej skuteczności wykrywania intruza, a także odporności na pobudzenia, których źródłem mogą być elementy wyposażenia lub zwierzęta znajdujące się w pomieszczeniu. Wiele modeli czujek umożliwia regulację czułości detekcji, która sprowadza się do ustawienia granicznego napięcia impulsu. Zadaniem instalatora jest dopasowanie ustawień czujki (czułości i liczby impulsów powodującej wysłanie sygnału alarmowego) do otoczenia i spodziewanego sposobu poruszania się intruza. Ustawienie zbyt niskiej czułości i zbyt dużej liczby impulsów daje dużo spokoju użytkownikowi, ale może być przyczyną braku alarmu w sytuacji, w której jest on potrzebny.

Okazuje się, że impulsy o jednakowej mocy i zbliżonej częstotliwości, pochodzące od pobudzeń z odmiennych źródeł mogą mieć zupełnie odmienne kształty. Wprawdzie w pomieszczeniach tylko w ekstremalnych przypadkach możemy spodziewać się temperatury otoczenia zbliżonej do temperatury człowieka, mierzonej z uwzględnieniem izolacji w postaci normalnej odzieży, ale temperatura powietrza nie jest dla czujki tak ważna jak temperatura tła – ścian, mebli, podłogi itd. Długotrwałe nagrzewanie pomieszczeń (lub – bardziej precyzyjnie – brak możliwości ich schładzania) powoduje, że czujka musi wykrywać minimalne różnice temperatury, co osłabia skuteczność jej działania. Zwiększanie czułości czujki zwiększa jej podatność na pobudzenia inne niż wywoływane przez ciało człowieka. Wielu producentów zaleca zastosowanie w takich warunkach dualnych czujek ruchu, w których analiza pasywnej podczerwieni wspomagana jest przez detekcję mikrofalową.

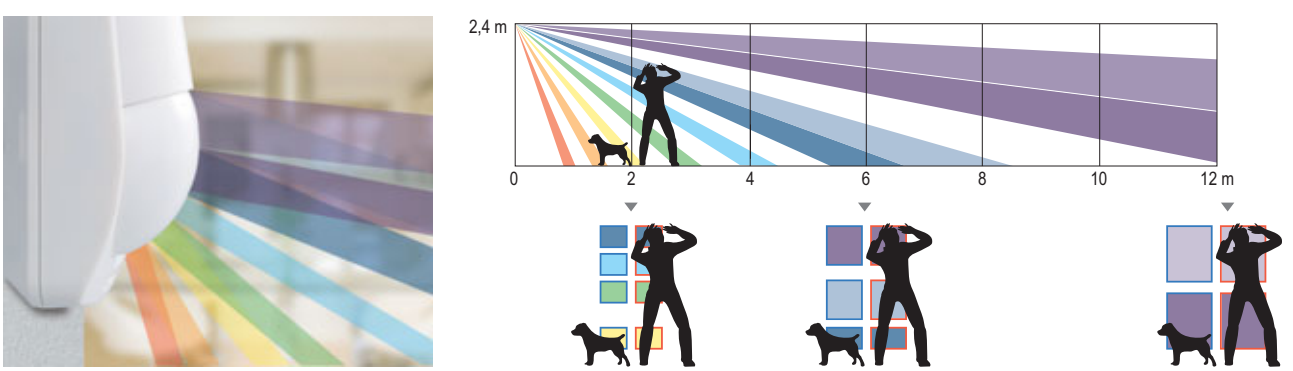
Przez dziesięciolecia swojej działalności firma OPTEX zdobyła duże doświadczenie w konstrukcji detektorów ruchu, które są przeznaczone do pracy na zewnątrz budynków, gdzie liczba czynników powodujących niepożądane pobudzenia jest wielokrotnie większa niż wewnątrz budynków. Nowatorskie rozwiązania wykorzystane w serii czujek HX-40 i HX-80 czy w zapowiadanym następcy klasycznego VX-402 – VX INFINITY stanowiły podstawę do opracowania algorytmu detekcji CORE dla nowych czujek wewnętrznych. Głębsza analiza przebiegu sygnału pochodzącego od znajdującego się w pomieszczeniu człowieka pokazuje, że ma on inny kształt niż sygnał generowany przez inne źródła zmiany promieniowania podczerwonego – grzejniki, klimatyzatory, poruszające się zasłony czy rośliny. Dlaczego więc nie porównywać tych kształtów i nie odrzucać pochodzących od zakłóceń?



Rys. 2. Algorytm CORE rozróżnia impulsy generowane przez różne źródła

Zamiast ulepszać sposób zliczania impulsów czy ustawiać ich amplitudy potrzebne do wywołania alarmu OPTEX opracował algorytm detekcji CORE analizujący kształt impulsu.

Firma OPTEX, korzystając z wiedzy i doświadczenia zdobytego dzięki tworzeniu urządzeń do detekcji zewnętrznej, stworzyła odpowiednią bazę danych, którą czujki wykorzystują podczas cyfrowej analizy sygnału. Zawiera ona wzorce impulsów charakterystycznych dla człowieka, zwierząt, grzejników i klimatyzatorów, poruszających się roślin czy zasłon,



Rys. 1. Podstawą analizy dokonywanej przez czujkę RXC wykorzystującą CORE jest sygnał z czterech precyzyjnie ukształtowanych i rozmieszczonych pól detekcji

ogrzewania podłogowego itd. Można powiedzieć, że algorytm CORE dokonuje jakościowej analizy sygnału w odróżnieniu od ilościowego zliczania impulsów.

Algorytm CORE dokonuje cyfrowej analizy źródła pochodzenia sygnału generowanego przez pyroelement. Elementy optyczno-mechaniczne, takie jak soczewka Fresnela generująca ponad 75 wiązek detekcji, szczelna obudowa zabezpieczająca przed owadami, układ kompensacji temperatury czy odpowiednio czuły pyroelement, mają za zadanie ułatwić pracę zespołowi sterującemu. Rozpoczęcie analizy jest uwarunkowane wystąpieniem sygnału na co najmniej czterech sąsiadujących polach detekcji. Ich kształt i rozmieszczenie są pierwszym etapem oceny wielkości intruza. W przeciwieństwie do wielu typów czujek przeznaczonych do systemów alarmowych montowanych w mieszkaniach zastosowany układ wiązek ułatwia też wykrywanie intruza poruszającego się w kierunku detektora. Nowy pyroelement jest lepiej dopasowany do charakterystyki pracy układu analizującego.

Zakłócenia elektryczne mogą wywoływać fałszywe alarmy. Zanim rozpocznie się analiza sygnału, układ filtracji zakłóceń rozpoznaje i eliminuje fragmenty impulsu będące wynikiem oddziaływania promieniowania elektromagnetycznego. Obecnie obowiązujące normy środowiskowe wymagają odporności na promieniowanie o częstotliwości do 2 GHz. Obecnie pomieszczenia mieszkalne, biurowe czy magazynowe są wyposażone w urządzenia komunikujące się bezprzewodowo, które wykorzystują wyższe częstotliwości, dlatego w normach, które będą obowiązywały od 2014 roku, wartość ta została podwyższona do 2,7 GHz. Czujki wyposażone w procesor z algorytmem CORE spełniają wymagania tych bardziej rygorystycznych norm.

Oprócz standardowych czujek RX-40QZ na rynku dostępna była wersja „SA", stosowana w krajach położonych na obszarach o cieplejszym klimacie, np. w południowej Europie, oraz wersja „PT", odporna na aktywność zwierząt domowych o wysokości do 40 cm. Algorytm CORE łączy zalety wszystkich modeli. Przełącznik ustawiony w położenie „HI" umożliwia pracę w wysokich temperaturach otoczenia. Ignorowanie przez czujkę obecności zwierząt domowych o wysokości do 40 cm uzyskujemy w położeniu „LOW", zaś w większości zastosowań pozostawiamy zworę w fabrycznym ustawieniu „MID". Nie trzeba ustawiać innych parametrów, takich jak zasięg czy liczba impulsów.

Kształt płyty sterowania czujkami RXC zaprojektowano tak, aby w takiej samej niewielkiej obudowie zmieścić również moduł mikrofalowy. Wymiana czujki podczerwieni na czujkę dualną może być dokonana bardzo szybko i łatwo bez jakiejkolwiek zmiany wystroju wnętrza.

Nowe czujki serii RXC spełniają wymagania dla stopnia 2. wg normy EN 50131, a wszystkie czujki serii CDX przeznaczone do zastosowań komercyjnych – wymagania dla stopnia 3. tej normy.

W ciągu ponad trzydziestu lat działalności firma OPTEX wprowadziła na rynek wiele innowacyjnych urządzeń. Celem działań badawczo-rozwojowych firmy jest skuteczność działania detektorów ruchu w najbardziej niesprzyjających warunkach, a technologia CORE jest kolejnym krokiem milowym w rozwoju firmy.

Jacek Wójcik
Optex Security

Security Products SINCE 1991 roger

seria radius

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.
- **INTEGRACJA** z innymi systemami:

RCP CCTV SSWiN

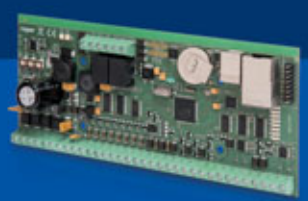
RCP Master *PR602LCD*

roger®

www.roger.pl

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Wprowadzono do oferty **CPR32-NET** – nową centralę systemu kontroli dostępu RACS 4 z interfejsem IP/Ethernet, umożliwiającą integrację z centralami alarmowymi INTEGRA oraz z zamkami mechatronicznymi serii SALLIS.



Mobilne aplikacje firmy SATEL

Michał Konarski

Nowoczesne centrale alarmowe umożliwiają nie tylko przekazywanie informacji o zagrożeniu. Dodatkową funkcją modułów komunikacyjnych może być na przykład zdalne sterowanie systemem alarmowym. Takie sterowanie jest ułatwione dzięki dynamicznemu rozwojowi smartfonów i tabletów, które można wyposażyć w odpowiednie oprogramowanie i które idealnie sprawdzają się w roli urządzeń sterujących

Wszechstronna komunikacja jest jedną z mocnych stron central z rodziny INTEGRA oferowanych przez firmę SATEL. Dzięki modułowi ETHM-1 można je podłączyć do Internetu i uzyskać zdalny dostęp do systemu w praktycznie każdym miejscu na świecie. Oczywiście jednym z priorytetów inżynierów z firmy SATEL, którzy stworzyli moduł zdalnego dostępu, było maksymalne zabezpieczenie urządzeń przed atakiem z sieci. Dlatego właśnie moduł ETHM-1 został wyposażony w wiele zabezpieczeń, takich jak szyfrowanie 192-bitowe czy ochrona przed atakami typu *brute force*.

Warto przy tym wspomnieć o rozbudowanych możliwościach central INTEGRA, które doskonale sprawdzają się w roli sterownika stanowiącego spójną całość z rozbudowanym systemem alarmowym w inteligentnym budynku. Dzięki tym możliwościom INTEGRĘ można wykorzystać np. do sterowania oświetleniem, klimatyzacją, wentylacją, podnoszeniem i opuszczaniem rolet czy nawet sterowania podlewaniem roślin.

Jedną z pierwszych stworzonych przez SATEL aplikacji do urządzeń mobilnych, które umożliwiają zdalne sterowanie centralami INTEGRA, jest MobileKPD. Aplikacja ta pozwala zamienić dowolny telefon z obsługą aplikacji Java ME w manipulator, dzięki któremu możliwe jest pełne sterowanie systemem alarmowym, dokładnie tak samo jak za pomocą tradycyjnej klawiatury. Dzięki MobileKPD można wpisywać polecenia na klawiaturze telefonu, a na jego ekranie pojawiają się informacje z systemu alarmowego.

Rosnąca popularność nowoczesnych telefonów z ekranami dotykowymi spowodowała, że opracowano aplikację wykorzystującą nowy sposób obsługi – MobileKPD2. Jest ona dostępna w wersjach dostosowanych do systemów operacyjnych iOS oraz Android, a także jako uniwersalna aplikacja Java,

Fot. 2. MobileKPD – aplikacja do nadzoru systemu bazującego na centralach INTEGRA

która może być uruchamiana na smartfonach z systemami Windows Mobile czy BadaOS. Obsługa systemu INTEGRA z wykorzystaniem MobileKPD2 Light jest dużo wygodniejsza niż z wykorzystaniem wcześniejszej wersji aplikacji. Usprawnienie wynika głównie z zastosowania łatwych w użyciu, dużych klawiszy ekranowych wirtualnego manipulatora i z czytelnego sposobu prezentowania informacji z systemu alarmowego. Aplikacja MobileKPD2 Light umożliwia zapamiętanie ustawień konfiguracyjnych dla wielu systemów alarmowych, dlatego można łatwo nawiązywać połączenia z różnymi systemami (np. w domu i w firmie), wybierając odpowiedni system w menu aplikacji.

Aplikacja MobileKPD2 Light pozwala korzystać ze wszystkich funkcji centrali INTEGRA – nie tylko z funkcji alarmowych, ale także z funkcji automatyki (inteligentnego budynku).

Fot. 1. Aplikacja MobileKPD2 dedykowana do telefononów z ekranami dotykowymi

Fot. 3. Przykładowe screeny z aplikacji MobileKPD2

Fot. 4. Aplikacja MobileKPD2 PRO posiada dodatkowo secjalne ekranowe przyciski funkcyjne umożliwiające szybkie uruchamianie nawet złożonych sekwencji

Fot. 5. Przykładowe screeny z aplikacji MobileKPD2 PRO

Bardziej złożone funkcje wymagają jednak nawigacji po menu centrali. Przykładowo – przy opuszczaniu rolet należy podać swoje hasło użytkownika, wybrać w menu funkcję sterowania wyjściami, a następnie wskazać odpowiednie wyjście na liście.

Jeśli korzystamy z bardziej rozbudowanych funkcjonalnie systemów INTEGRA, najlepiej stosować aplikację MobileKPD2 PRO.

Fot. 6. Aplikacja MICRA CONTROL jest przeznaczona do zdalnego sterowania systemem alarmowym MICRA

Fot. 7. Przykładowe screeny z aplikacji MICRA CONTROL

W jej przypadku wirtualny manipulator INTEGRA ma dodatkowo specjalne ekranowe przyciski funkcyjne umożliwiające szybkie uruchamianie nawet złożonych sekwencji. Dzięki możliwości skonfigurowania funkcji tych przycisków można je wykorzystać na przykład do łatwego sterowania urządzeniami automatyki, np. do sterowania podnoszeniem i opuszczaniem rolet, włączaniem i wyłączaniem świateł czy nawet do wydawania całych sekwencji pojedynczych poleceń ujętych w scenariusze. W ten sposób aplikacja MobileKPD2 PRO zamienia smartfona lub tablet we wszechstronny i rozbudowany sterownik inteligentnej instalacji, której rdzeń stanowią centrale z rodziny INTEGRA.

Olbrzymie zainteresowanie oprogramowaniem z funkcjami zdalnego sterowania systemem alarmowym, skłoniło firmę SATEL do opracowania kolejnej aplikacji. Najnowsza propozycja skierowana jest do właścicieli obiektów, które często pozostawiane są bez ciągłego nadzoru (np. domków letniskowych, placów budowy, garaży, warsztatów). Aplikacja MICRA CONTROL pozwala sterować systemem z modułem alarmowym MICRA. Umożliwia wykorzystanie smartfonów z systemem operacyjnym Android nie tylko do włączania i wyłączania czuwania, ale także do sterowania wyjściami modułu oraz blokowania wejść. Do sterowania wykorzystywane są SMS-y. MICRA CONTROL umożliwia też sprawdzenie aktualnego stanu systemu. Dodatkowym dużym atutem tej aplikacji jest efektowny interfejs użytkownika, dzięki któremu korzystanie z narzędzia jest nie tylko łatwe, ale także przyjemne.

Dostępność narzędzi umożliwiających interaktywną, zdalną obsługę urządzeń alarmowych lokuje produkty SATEL w ścisłej światowej czołówce. Warto po nie sięgnąć, gdyż oferują wymierne korzyści użytkownikowi systemu – ułatwiają codzienną obsługę i mają funkcje, które dotychczas nie były dostępne w popularnych centralach alarmowych. Dodatkowym atutem jest możliwość sprawdzenia stanu systemu w dowolnym miejscu i czasie.

Michał Konarski
SATEL

Systemy alarmowe **Satel**

Zdalne sterowanie systemem

Aplikacja oferuje atrakcyjny wizualnie i prosty w obsłudze interfejs, za pomocą którego możliwe jest:

- **włączanie i wyłączanie czuwania**
- **sprawdzanie stanu systemu**
- **sterowanie wyjściami**
- **blokowanie wybranych wejść**

Nowa aplikacja **MICRA CONTROL** to bardzo duże ułatwienie dla użytkownika w codziennym sterowaniu systemem **MICRA**.

Dużą zaletą aplikacji MICRA CONTROL jest funkcja automatycznej konfiguracji. Wystarczy podać numer telefonu karty SIM w module MICRA, aby aplikacja samoczynnie skonfigurowała odpowiednie ustawienia zgodnie z ustawieniami zapisanymi w module. Aplikacja dostępna jest dla urządzeń mobilnych z systemem Google Android.

Satel Sp. z o.o.
ul. Franciszka Schuberta 79, 80-172 Gdańsk, tel.: (58) 320 94 00, fax: (58) 320 94 01, e-mail: satel@satel.pl **www.satel.pl, www.mieszkajbezpiecznie.pl**

JABLOTRON 100

innowacyjne rozwiązanie dla bezpiecznego i inteligentnego domu

Tomasz Leopold

Nowy, hybrydowy system alarmowy czeskiego producenta – JABLOTRON 100 – wchodzi na polski rynek i zyskuje uznanie. Innowacyjne rozwiązania w tym systemie spełnią oczekiwania zarówno specjalistów z branży, jak i nabywców

Bezpieczeństwo i komfort obsługi

Jakie założenia przyświecały projektantom systemu JABLOTRON 100? Z pewnością chcieli stworzyć inteligentny system, który zarazem zabezpieczy obiekt i umożliwi zarządzanie nim, czyli będzie stanowił połączenie systemu alarmowego i automatyki budynkowej. Uwzględniono również to, że użytkownicy oczekują prostoty obsługi urządzeń i możliwości indywidualnego dopasowania systemu do obiektu. Efektem ich pracy jest system JABLOTRON 100.

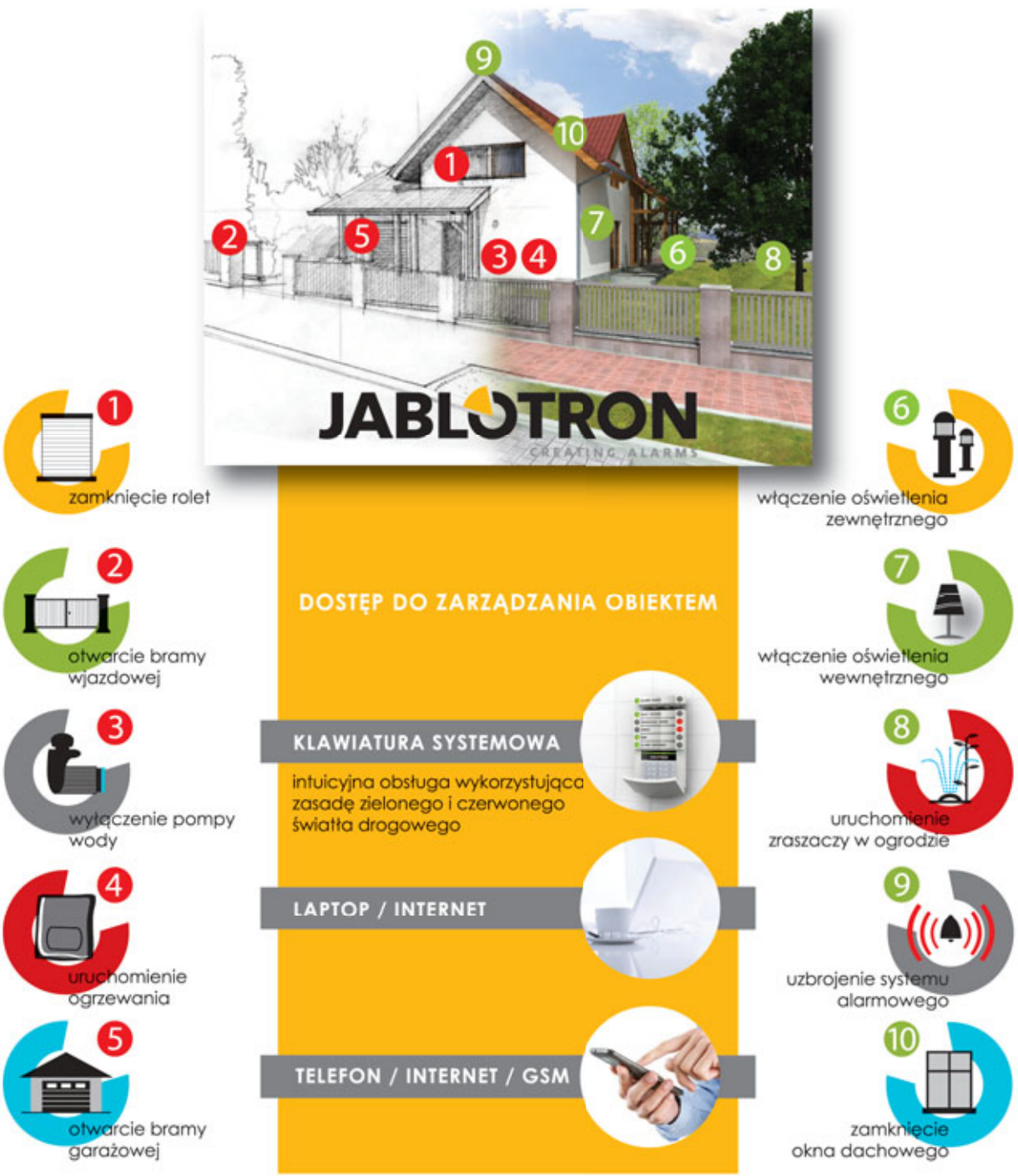
Parametry techniczne systemu

Hybrydowy system JABLOTRON 100 to innowacyjne podejście do zadań kontroli dostępu i sterowania. Producent dołożył wszelkich starań, aby nowy system był jeszcze bardziej funkcjonalny, intuicyjny i przyjazny w obsłudze w porównaniu ze starszymi systemami z serii Profi i Oasis.

Podstawowymi elementami systemu JABLOTRON 100 są centrale sterujące JA-101K oraz JA-106K. Można je przystosować zarówno do małych, jak i średniej wielkości instalacji. Dzięki temu system znakomicie sprawdzi się w mieszkaniach, domach, biurach, sklepach, obiektach handlowych lub produkcyjnych.

Właściwości pojedynczej centrali JA-101K:

– możliwość przyłączenia 50 urządzeń bezprzewodowych lub przewodowych do magistrali cyfrowej BUS,
– do 50 rozróżnialnych użytkowników,
– do 6 niezależnych sekcji (stref),
– do 8 programowanych wyjść PG,



Rys. 1. Automatyka domowa – przykłady zdarzeń

– 20 programowanych zdarzeń z kalendarza,
– raporty o zdarzeniach wysyłane do 8 użytkowników w postaci wiadomości SMS,
– raporty o zdarzeniach wysyłane do 5 użytkowników w postaci wiadomości SMS oraz komunikatu głosowego,
– wysyłanie raportów do 4 stacji monitorowania ARC,
– 5 opcji wyboru raportów do ARC.

Właściwości pojedynczej centrali JA-106K:
– możliwość podłączenia 120 urządzeń bezprzewodowych lub przewodowych do magistrali cyfrowej BUS,
– do 300 rozróżnialnych użytkowników,
– do 15 niezależnych sekcji (stref),
– do 32 programowanych wyjść PG,
– 20 programowanych zdarzeń z kalendarza,
– raporty o zdarzeniach wysyłane do 30 użytkowników w postaci wiadomości SMS,
– raporty o zdarzeniach wysyłane do 5 użytkowników w postaci wiadomości SMS oraz komunikatu głosowego,
– wysyłanie raportów do 4 stacji monitorowania ARC,
– 5 opcji wyboru raportów do ARC.

Każda centrala ma wbudowany komunikator GSM/GPRS, a centrala JA-106K – również komunikator LAN. Do archiwizacji wszystkich zdarzeń, komunikatów głosowych oraz zdjęć służy karta pamięci o pojemności 1 GB, gwarantująca pięcioletni okres archiwizacji.

Szczegółowe raporty zdarzeń

Bardzo ważnym atutem systemu JABLOTRON 100 jest rozbudowany system raportowania, dzięki któremu zawsze otrzymujemy pełną informację o danym zdarzeniu. W raporcie podawane są: nazwa obiektu, data i godzina zdarzenia, rodzaj zdarzenia, dokładne miejsce zdarzenia i jego źródło. Przykładowe raporty: dom/ul. Grota Roweckiego 14/14.02.2012/godz. 13^{24}/alarm linia nagła/czujnik – garaż; firma/ul. Poznańska 2/25.05.2012/godz. 11^{05}/alarm linia sabotażowa/czujnik biuro; apartament/ul. Marcelińska 9/06.11.2012/godz. 18^{00}/oświetlenie zewnętrzne/załączone.

*– Centrale JABLOTRON 100 umożliwiają adaptację systemu zarówno w małych, jak i dużych obiektach. Hybrydowość to idealne rozwiązanie w przypadku projektów, w których trzeba elastycznie połączyć urządzenia przewodowe i bezprzewodowe. Cenną zaletą systemów JABLOTRON jest również ich bezproblemowa obsługa serwisow*a – zauważa Arkadiusz Tokarski – prezes Alles S.C.

Automatyka domowa w przystępnej cenie i bez skomplikowanej instalacji

System automatyki dla domu nie musi być skomplikowany i drogi. JABLOTRON 100 gwarantuje skonfigurowanie automatyki domowej zgodnie z potrzebami i preferencjami użytkownika. Instalacja może zostać wykonana w technice przewodowej, z wykorzystaniem magistrali BUS, oraz bezprzewodowej, co umożliwia przyłączenie elementów wykonawczych przy bardzo prostej instalacji. Cała instalacja może zostać zbudowana

– JABLOTRON 100 ma wiele funkcji i oferuje dużo możliwości konfiguracji. Obserwujemy bardzo duże zainteresowanie systemem. JABLOTRON 100 umożliwia łatwą i szybką instalację, a także intuicyjną obsługę. Jest to bardzo ważne dla użytkownika systemu – twierdzi Piotr Siarno – prezes Teleconnections.

bezprzewodowo lub z użyciem jednego przewodu CC-01 (2×0,5 + 2×0,8 [mm]) albo CC-02 (4×0,5 mm). Centrala systemu JABLOTRON 100 obsługuje do 32 wyjść programowanych – czyli mamy 32 niezależne działania, które możemy wykonać. Co ważne, do każdego wyjścia możemy przypisać praktycznie nieograniczoną liczbę elementów wykonawczych, gdyż w odbiorniku elementu wykonawczego zostaje doń przypisane konkretne wyjście PG. Odbiornikami można sterować za pomocą klawiatury lub pilotów. Użytkownik mający dostęp do Internetu może zarządzać systemem zdalnie – poprzez serwis *www.jablonet.net* lub poprzez aplikację F-Link. Dzięki takim rozwiązaniom możemy bezproblemowo zarządzać swoim obiektem niezależnie od tego, gdzie się znajdujemy.

Niezliczone możliwości konfiguracji

Konfigurowanie systemu JA-100 jest dla instalatora łatwe. Warto zauważyć, iż oprogramowanie F-Link daje mnóstwo możliwości konfiguracji systemu pod kątem zależności jednej reakcji od drugiej. Przykłady wykorzystania tych zależności moglibyśmy wymieniać długo. Jednym z nich może być naruszenie zewnętrznego czujnika zbicia szkła wywołujące alarm i zarazem powodujące włączenie

– Obserwujemy coraz większe zainteresowanie systemami alarmowymi połączonymi z elementami automatyki domowej. Klienci szukają urządzeń nowoczesnych, ale zarazem łatwych w obsłudze. Systemy JABLOTRON spełniają obydwa te warunki. Widzimy, że instalatorzy doceniają łatwą, nieinwazyjną instalację tych systemów, a użytkownicy łatwość obsługi urządzeń – podkreśla Rafał Kozelan, kierownik Działu Zabezpieczeń Anmar.

oświetlenia zewnętrznego i zamknięcie rolet elektrycznych. Inny przykład – w momencie wykrycia wycieku wody przez czujnik zalania odbiornik PG spowoduje zakręcenie elektrozaworu i odcięcie dopływu wody. Istnieje również możliwość wyznaczenia zadań, które system ma wykonać w określonym terminie. Może to być na przykład uruchomienie zraszacza lub włączenie oświetlenia w ogrodzie. System może nas poinformować o wystąpieniu danej zależności poprzez wiadomość SMS, MMS, e-mail lub komunikator głosowy.

Tomasz Leopold
JabloTech

Nie uciekniemy od biometrii

Rozmowa z prof. dr hab. inż. Andrzejem Pacutem, kierownikiem Zespołu Biometrii i Uczenia Maszynowego w Instytucie Automatyki i Informatyki Stosowanej Politechniki Warszawskiej

Banki coraz częściej wprowadzają techniki biometryczne, aby lepiej chronić dane oraz pieniądze swoich klientów. Na czym polega skuteczność biometrii w tego typu zastosowaniach?
A. P.: Zauważmy, że wszelkiego rodzaju klucze, karty czy kody mogą zostać wykorzystane przez osoby nieuprawnione. Dzięki zabezpieczeniom biometrycznym można zweryfikować tożsamość osoby próbującej uzyskać dostęp.

Politechnika Warszawska uruchomiła w zeszłym roku studia podyplomowe[1] dotyczące bezpieczeństwa informacyjnego i technik biometrycznych. Jak duża jest potrzeba wprowadzania takich kierunków i czego mogą nauczyć się słuchacze?
A. P.: Techniki biometryczne są już obecne w polskiej rzeczywistości. Oczywiście od dawna są stosowane w ekspertyzach sądowych. Zabezpieczeniem biometrycznym mogą być podpisy składane na specjalnych tabletach, umożliwiające automatyczną weryfikację. Biometrycznie zabezpieczane są paszporty. W kolejce czekają systemy identyfikacji telefonującego na podstawie głosu w działach obsługi klienta. Zabezpieczenia biometryczne stosowane są również w komputerach, pamięciach przenośnych, a także do ochrony pomieszczeń. Można podać szereg innych przykładów z różnych odległych dziedzin. Wszystko wskazuje na to, że urządzenia biometryczne będą wykorzystywane na coraz szerszą skalę. Studia dotyczące bezpieczeństwa i technik biometrycznych, proponowane przez Wydział Elektroniki i Technik Informacyjnych PW, włączają zagadnienia związane z biometrią do całokształtu zagadnień związanych z bezpieczeństwem. Znajomość podstaw biometrii umożliwi właściwe jej wykorzystanie, zrozumienie możliwych błędów i pułapek.

Biometria przynosi wiele korzyści, ale budzi jeszcze wiele emocji i kontrowersji...
A. P.: Biometria rzeczywiście budzi wiele emocji. Niektórzy obawiają się przejęcia danych biometrycznych. Do metod biometrycznych należy między innymi rozpoznawanie tożsamości na podstawie obrazu twarzy, głosu czy podpisu odręcznego. Podpis odręczny pozostawiamy na ważnych dokumentach, jednak warto zauważyć, że nie obawiamy się zbytnio, że zostanie on skopiowany czy sfałszowany – liczymy na inne, współwystępujące zabezpieczenia. Twarz wystawiamy ciągle na widok publiczny. Obecnie stosowane są bardzo zaawansowane zabezpieczenia biometryczne, np. bazujące na obrazie tęczówki czy też obrazie naczyń krwionośnych. Wzorce biometryczne są w specjalny sposób zabezpieczane przed ponownym użyciem w przypadku wykradzenia ich z bazy danych. Sporo obaw budzi rozszerzenie możliwości pomiarowych, rozwijanie technik rozpoznawania bez zgody i wiedzy osoby obserwowanej i związana z tym możliwość inwigilacji, która jest ułatwiona dzięki szybkiemu i automatycznemu przetwarzaniu danych. Związane z tym zagadnienia prawne, problemy społeczne, obyczajowe i religijne, a także związane z nimi ograniczenia stosowania technik biometrycznych są również omawiane na naszych wykładach.

Jaka jest Pana zdaniem przyszłość biometrii?
A. P.: Biometria ma zastosowanie wszędzie tam, gdzie istotne jest potwierdzenie lub rozpoznanie tożsamości. Obszar jej możliwych zastosowań jest ogromny. W 2009 roku całkowite dochody ze sprzedaży i licencjonowania produktów i usług biometrycznych wyniosły 3,5 miliarda USD. Według *Biometrics Market and Industry Report 2009–2014* w 2014 roku, mimo kryzysu, znacznie przekroczą 9 miliardów USD. Na rynek biometryczny wchodzą nowe technologie. Gwałtownie rozwinęły się i są stosowane techniki oparte na wzorze naczyń krwionośnych. Rozwój technik wizyjnych i metod analizy obrazu pozwala na rozpoznawanie twarzy ze znacznej odległości. Rozwijają się także techniki rozpoznawania na podstawie trójwymiarowego obrazu twarzy. Szybko wchodzą na rynek techniki wykorzystujące badania DNA – chodzi o szybkość, dostępność i koszt pomiarów. Równocześnie dane są coraz lepiej zabezpieczane, a dane biometryczne są coraz trudniejsze do sfałszowania. Bezpieczeństwo w wielu dziedzinach będzie zależeć od biometrii. Od tego już nie uciekniemy.

1) Studia są organizowane przez Politechnikę Warszawską i przeznaczone dla specjalistów w dziedzinie bezpieczeństwa oraz osób, które chcą zawodowo zajmować się bezpieczeństwem informacyjnym. Więcej informacji o studiach można znaleźć na stronie www.BezpieczenstwoBiometria.org.pl.

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

ipGO

Nowa rodzina produktów **do monitoringu wizyjnego IP**

Nie jesteś przekonany do technologii IP?

Ten system zmieni Twoje myślenie o urządzeniach sieciowych!

Zero problemów z podłączaniem kamer

100% zadowolenia z doskonałej jakości obrazu

Sprawdź, co potrafi ipGO!

- AUTONOMICZNY SYSTEM
- AUTOMATYCZNA KONFIGURACJA
- OBRAZ Full HD
- PODGLĄD NA SMARTFONACH
- PROSTA OBSŁUGA
- NOWOCZESNY DESIGN

Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Automatyczna konfiguracja całego systemu

ipGO **To takie proste!**

NVIP-NVRA0104/GO
NVIP-NVRA0208/GO

NVIP-2C2001D-P/GO

NVIP-2C5005CZ-P/GO

System ipGO pracuje zgodnie ze standardem Plug & Play, czyli jest gotowy do działania od razu po podłączeniu. Dzięki temu instalacja systemu jest bardzo prosta i zajmuje tyle samo czasu, co zamontowanie systemu analogowego.

1... 2... 3... i gotowe! System działa!

Podłączamy kamerę...

... do odpowiedniego portu w rejestratorze sieciowym ...

... i system jest gotowy do pracy!

Doskonała jakość obrazu Full HD Liczą się szczegóły!

Sceny kamery analogowej

Kamery ipGO

Zdalny dostęp do obrazu z kamer za pomocą urządzeń mobilnych !

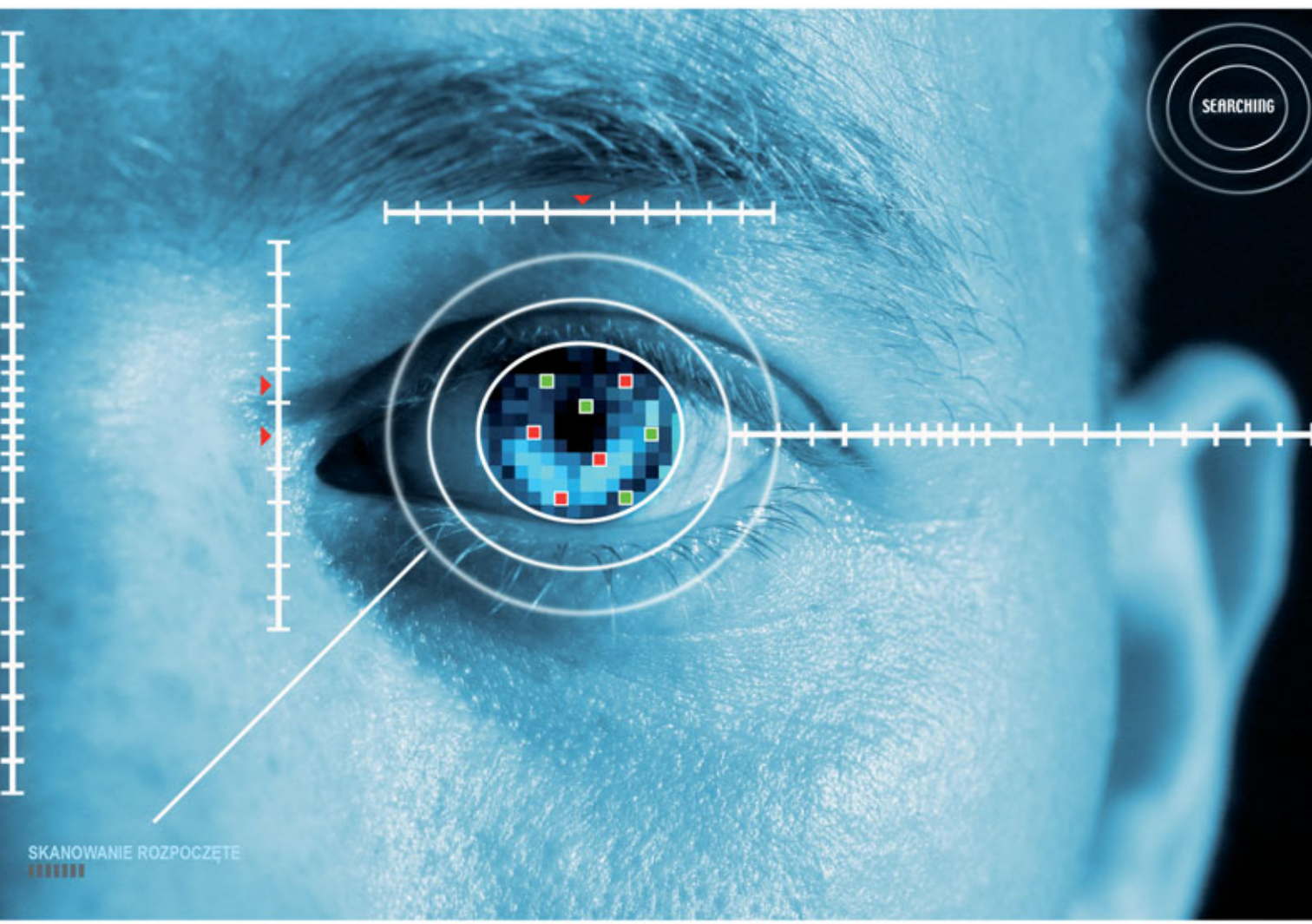
iPhone Compatible

Android Compatible

Biometria w kontekście problemów prawnych

Monika Brzozowska

Biometria i związane z nią problemy (zarówno techniczne, jak i prawne) to ostatnio coraz modniejszy temat do debat. Wykorzystywanie jej na co dzień to nie futurystyczna wizja, ale rzeczywistość, zatem warto przedstawić związane z nią uregulowania prawne



Za biometrię uważa się zbiór technik służących do pomiarów cech fizycznych i behawioralnych człowieka w celu automatycznej weryfikacji tożsamości. Sprawdza się m.in. barwę głosu, zapach, linie papilarne układ naczyń krwionośnych palców, geometrię dłoni, geometrię i rysy twarzy, rozkład temperatury twarzy, fakturę skóry twarzy, geometrię ucha, geometrię ust, cechy charakterystyczne tęczówki i siatkówki oka, układ żył nadgarstka, strukturę włosów i paznokci, EEG, ECG, DNA. Do sprawdzanych cech behawioralnych należy głos, sposób mówienia, sposób poruszania ustami, ruch gałki ocznej, charakter pisma, sposób pisania na klawiaturze, sposób chodzenia.

Wśród prawników oraz informatyków nie brakuje zwolenników oraz przeciwników wykorzystywania biometrii w życiu codziennym. Entuzjaści uznają ją za najbezpieczniejsze i najwygodniejsze narzędzie służące do weryfikacji tożsamości i uprawnień. Przeciwnicy zwracają uwagę na możliwość ingerencji w prawa człowieka, a także na fakt, że w dobie nowych technologii dane biometryczne łatwo sfałszować. Zdaniem przeciwników biometrii gromadzenie i przetwarzanie danych

biometrycznych może naruszać prawa obywateli. Podkreśla się bowiem, że dane te – jako odnoszące się do cech behawioralnych i fizjologicznych – umożliwiają absolutną identyfikację osób. Ponadto możliwe jest ich sfałszowanie, które może mieć groźne konsekwencje. Przykładowo, w 2010 r. na Politechnice Warszawskiej w ramach ćwiczeń laboratoryjnych studenci stworzyli sztuczne odciski palców. Podobno wystarczyło zrobić zdjęcie odcisków czyichś palców, np. zostawionych na szklance, i wydrukować je na folii. Barwnik drukarki na folii tworzy nierówności analogiczne do odcisków palców. Taką folię wystarczy pokryć odpowiednią kleistą substancją i mamy gotowy odcisk palca. Podobnie jest z tęczówką oka, do sfałszowania której potrzebne jest tylko zdjęcie oka o rozdzielczości 3 Mpx.

Same dane biometryczne nie są zdefiniowane wprost w ustawie o ochronie danych osobowych, jeśli jednak odpowiadają one przesłance z art. 6 tej ustawy (dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgodnie z ust. 2 i 3 art. 6), będą chronione na podstawie tego aktu prawnego. Brak legalnej definicji biometrii i danych biometrycznych w ustawie o ochronie danych osobowych nie oznacza, że w polskim lub unijnym ustawodawstwie takich definicji nie ma. Pojęcie danych biometrycznych pojawia się w ustawie o dokumentach paszportowych, która definiuje je jako wizerunek twarzy i odciski palców umieszczone w dokumentach paszportowych w formie elektronicznej (art. 2 pkt 1). Zgodnie z tą ustawą sporządzeniem dokumentu paszportowego jest przeniesienie danych osobowych i biometrycznych osoby ubiegającej się o wydanie dokumentu paszportowego do książeczki paszportowej w postaci graficznej i elektronicznej (art. 2 pkt 4). Definicja przedstawiona w ustawie o dokumentach paszportowych jest dość wąska, gdyż rodzajów danych biometrycznych jest więcej.

W prawie unijnym kwestie związane z danymi biometrycznymi są regulowane przez rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, w którym za dane biometryczne uznaje się wyraz twarzy oraz odcisk palców (art. 1 ust. 2).

Sama ustawa o ochronie danych osobowych zalicza do grupy danych wrażliwych m.in. informacje o kodzie genetycznym, co oznacza, że w większości przypadków dane biometryczne będą traktowane jako wrażliwe, w związku z czym będą się do nich odnosić wszystkie zasady dotyczące danych wrażliwych. Przy ich przetwarzaniu będzie więc potrzebny podwyższony poziom zabezpieczenia (jeśli żaden z komputerów przetwarzających dane biometryczne nie będzie podłączony do sieci publicznej) albo wysoki poziom zabezpieczenia (jeśli co najmniej jeden komputer będzie podłączony do sieci publicznej). Co więcej, zgoda na przetwarzanie tego typu danych będzie musiała być wyrażona na piśmie. W przeciwnym razie będzie nieważna. Brak zgody nie będzie uniemożliwiał przetwarzania takich danych, jednakże ich przetwarzanie będzie musiało odbywać się na podstawie przesłanek określonych w art. 27 ustawy o ochronie danych osobowych, które są mocno rygorystyczne.

Wprowadzanie danych biometrycznych do dokumentów wiąże się z wieloma konsekwencjami. Słusznie sugeruje się, że nie można zapominać o ochronie prywatności.

W dniu 30 września 2005 r. przyjęto opinię 3/2005 Grupy Roboczej Art. 29 ds. Ochrony Danych pod tytułem *Dokument roboczy w sprawie biometrii*, która dotyczyła wprowadzenia w życie rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie. Grupa robocza ustosunkowała się następująco: „Wprowadzenie elementów biometryki do paszportów wiąże się z daleko idącymi konsekwencjami dla ich posiadaczy. Dlatego też nie powinno się go dokonywać bez uprzedniej oceny wpływu na ochronę prywatności. Dotychczas wystarczającymi odniesieniami do cech biometrycznych odnotowanymi w paszportach i innych dokumentach podróży były zdjęcia, określenie płci, wzrostu czy koloru oczu. Po wejściu w życie rozporządzenia Rady (WE) nr 2252/2004 dane biometryczne obywateli przybiorą formę cyfrową. Dane te można będzie przechowywać w bazach danych i będą mogły być udostępniane do wielu nieprzewidywalnych celów". *Dokument roboczy w sprawie biometrii* pochodzi z 2005 r., jednak wydaje się nadal aktualny.

Wykorzystywanie danych biometrycznych (zarówno w sferze prywatnej, jak i publicznej) powinno być poprzedzone stworzeniem odpowiednich zabezpieczeń przed nieuprawnionym dostępem. Dane biometryczne uznaje się za wrażliwe, dlatego ich przetwarzanie i zabezpieczanie powinno być identyczne jak przetwarzanie i zabezpieczanie danych wrażliwych. Biometria ma swoich zwolenników i przeciwników. Warto zastanowić się nad stanowiskiem, zgodnie z którym zastosowanie biometrii stwarza ryzyko nadużyć, przestępstw, naruszenia prywatności i godności.

Adwokat Monika Brzozowska

Autorka jest Partnerem w kancelarii PDB LEGAL Pasieka, Derlikowski, Brzozowska i Partnerzy, specjalistą zajmującym się na co dzień problematyką ochrony dóbr osobistych i danych osobowych, prawami autorskimi oraz prawnymi aspektami funkcjonowania cyberprzestrzeni. Jest także ekspertem Instytutu Sobieskiego.

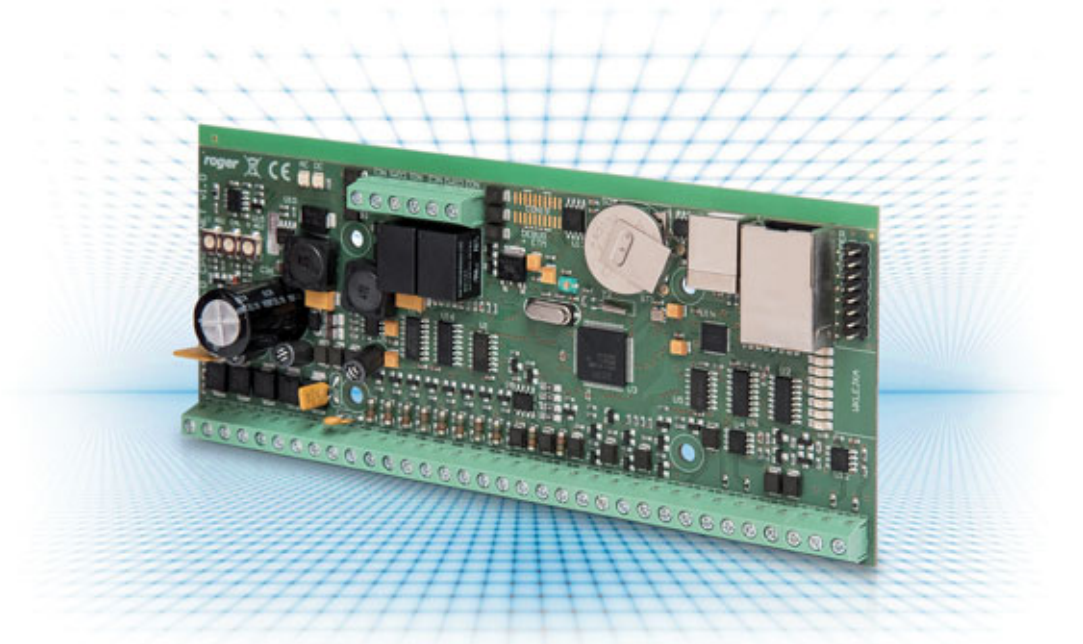
Od redakcji

Poruszone w artykule prawne aspekty wykorzystania danych biometrycznych w różnych dziedzinach dotyczą nie tylko kontroli dostępu, ale również gromadzenia i przechowywania takich danych w celach ewidencyjnych, np. w kartotekach policyjnych.

Inne przykładowe zastosowanie, przedstawione w niniejszym artykule, to umieszczenie ich w paszportach biometrycznych. Dane biometryczne pozyskiwane i przechowywane w systemach kontroli dostępu mają inną specyfikę. Ze względu na ograniczoną pamięć czytników biometrycznych oraz wymaganą dużą szybkość procesu automatycznej identyfikacji osoby na kontrolowanym przejściu pozyskane dane biometryczne są przetwarzane na stosunkowo niewielki ciąg binarny za pomocą specjalnego algorytmu. Z wytworzonego w taki sposób ciągu nie można odtworzyć kompletnego obrazu linii papilarnych palca. Takie „dane biometryczne" nie są porównywalne z ilością informacji zawartą w kompletnym obrazie odcisku palca przechowywanym w bazie policji, dlatego, mówiąc o danych biometrycznych, należy zawsze brać pod uwagę to, co jest finalnie przechowywane i wykorzystywane w danym zastosowaniu.

Centrala CPR32-NET

Centrala systemu kontroli dostępu RACS 4 z interfejsem IP/Ethernet



Centrala CPR32-NET stanowi kolejną, rozwojową wersję oferowanej od kilku lat centrali kontroli dostępu typu CPR32-SE. Ten nowy produkt realizuje wszystkie funkcje swojego poprzednika, a dodatkowo oferuje szereg nowych możliwości, z których najważniejsze to możliwość programowej integracji z centralami alarmowymi INTEGRA (wymagany jest interfejs INT-RS) oraz możliwość współpracy z zamkami mechatronicznymi serii SALLIS (firmy SALTO). Zrealizowana w centrali CPR32-NET koncepcja integracji z centralami INTEGRA polega na możliwości sterowania uzbrojeniem stref alarmowych, zarówno z poziomu manipulatorów systemu alarmowego jak i czytników systemu kontroli dostępu. Ponadto system kontroli dostępu pobiera i wyświetla w swoim logu zdarzeń pewne krytyczne zdarzenia pochodzące z systemu alarmowego w wyniku czego operator systemu może się ograniczyć do monitorowania jednego wspólnego logu zdarzeń. Nowa centrala oferuje także opcję zapisu zdarzeń na wymiennej karcie pamięci FLASH co powoduje, że zastosowanie odpowiednio dużej karty pamięci może w praktyce zabezpieczyć bufor zdarzeń na kilka lat pracy systemu bez zagrożenia jego przepełnieniem. Komunikacja z nową centralą odbywa się przez sieć LAN/WAN z wykorzystaniem standardu szyfrowania AES 128.

Charakterystyka

- Obsługa systemu złożonego z maks. 32 kontrolerów serii PR
- Osiem wejść parametrycznych
- Sześć wyjść tranzystorowych 15 V_{DC}/1 A
- Dwa wyjścia przekaźnikowe 30 V/1,5 A
- Zarządzanie harmonogramami czasowymi i kalendarzami
- Wbudowany interfejs komunikacyjny IP/Ethernet
- Szybka, szyfrowana transmisja danych pomiędzy centralą a komputerem zarządzającym
- Wbudowany nieulotny bufor pamięci o pojemności 250 tys. zdarzeń z możliwością rozszerzenia o dodatkową kartę pamięci
- Realizacja funkcji globalnych (Strefy Alarmowe, Globalny Antipassback itd.)
- Integracja programowa z centralami alarmowymi Integra (firmy SATEL)
- Integracja programowa z zamkami mechatronicznymi Sallis (firmy SALTO)
- Zasilanie 18 V_{AC} lub 12 V_{DC}
- Wbudowany zasilacz impulsowy z wyjściem 12 V_{DC}/1 A
- Aktualizacja oprogramowania wbudowanego (firmware)

Producent: roger®

Roger Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

PR612/PR622

Nowe kontrolery dostępu serii zaawansowanej

Kontrolery PR612 oraz **PR622** firmy Roger są następcami popularnego kontrolera PR302. Oba urządzenia posiadają wbudowany czytnik standardu EM 125 kHz, zegar czasu rzeczywistego oraz bufor pamięci do rejestracji zdarzeń występujących w systemie kontroli dostępu. Kontrolery PR612 i PR622 mogą być stosowane jako autonomiczne punkty kontroli dostępu lub tworzyć sieć w ramach systemu kontroli dostępu RACS 4 obejmującego różne kontrolery pojedynczego przejścia.

Charakterystyka

- Jedno lub dwustronna kontrola drzwi
- Możliwość dołączenia czytnika serii PRT (Roger) w celu obustronnej kontroli przejścia
- Obsługa do 4000 użytkowników
- Bufor pamięci na 32 000 zdarzeń
- Zasilanie z 12 V_{DC}
- Trzy wejścia NO/NC
- Dwa wyjścia tranzystorowe 15 V_{DC}/1 A
- Wyjście przekaźnikowe 30 V/1,5 A
- Wbudowana klawiatura numeryczna (tylko PR612)
- Wbudowany głośnik
- Możliwa praca w warunkach zewnętrznych
- Ochrona antysabotażowa (tamper)
- Komunikacja przez RS485 z zastosowaniem dowolnej topologii magistrali komunikacyjnej
- Funkcje typu wejście komisyjne, wejście warunkowe, losowa kontrola użytkowników i inne
- Integracja z systemami alarmowymi, systemami rejestracji czasu pracy oraz telewizją przemysłową
- Tryby drzwi: normalny, zablokowane, odblokowane i warunkowo odblokowane
- Tryby identyfikacji: karta lub PIN, karta i PIN, tylko karta, tylko PIN
- Kontrola dostępu w windach (wymagany moduł XM-8)

Producent: roger®

Roger Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

Kamera DBD-51VD

Kamera **DBD-51VD** należy do nowej rodziny kamer CNB bazujących na procesorach DSP Effio firmy Sony oraz posiadających rozdzielczość aż 700 TVL. W DBD-51VD zastosowano DSP Enhanced Effio-E, który jest unowocześnioną wersją Effio-E.

DBD-51VD to kamera do zastosowań wewnętrznych gdzie wymagamy poszerzonej dynamiki ATR, czy innych funkcji np. DNR, BLC i HLC. ATR czyli Adaptive Tone Reproduction to autorskie rozwiązanie DWDR firmy Sony w DSP Effio. ATR to funkcja zwiększająca kontrast i czytelność, rozjaśnia zbyt ciemne partie obrazu, nie prześwietlając jasnych.

Zalety

- Wbudowany obiektyw o zmiennej ogniskowej 3,8÷9,5 mm z automatyczną przysłoną
- Dodatkowe wyjście wizyjne dla instalatora
- Regulacja położenia modułu kamery w 3 osiach: pion, poziom oraz obrót wokół własnej osi
- Funkcje BLC i HLC - możliwość lepszej obserwacji scen o zróżnicowanej jasności
- Funkcja ATR - poprawa dynamiki kamery

Właściwości

- Kolorowa kamera dzień/noc
- Przetwornik 1/3" SONY 960H CCD
- Bardzo wysoka rozdzielczość 700 TVL
- Automatyczne przełączanie się kamery w tryb B/W
- Czułość 0,05 lx (kolor), 0,01 lx (B/W)
- Obiektyw 3,8÷9,5 mm DC
- Menu ekranowe
- Regulacje jasności oraz koloru obrazu
- Funkcje AGC, ATR, BLC, HLC, AWB, DNR, Flickerless, D/N – regulacja przez menu ekranowe
- Funkcje detekcji ruchu, stref prywatności, odwracania obrazu, wyostrzanie obrazu
- Zasilanie 12 V_{DC}
- Obudowa kopułkowa o średnicy 120 mm

Standard sygnału wizyjnego	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY 960H CCD
Rozdzielczość efektywna	976(H) x 582(V) 570k
Liczba linii telewizyjnych	700 TVL
Wyjście wizyjne	1,0V p-p, 75 Ohm
Obiektyw	3,8÷9,5 mm DC
Odstęp sygnał/szum	>50dB
Sposób mocowania obiektywu	mocowanie CS
Filtr IR	stały
Czułość	0,05 Lux (kolor), 0,01 lx (B/W), F1.2, przy 30IRE
Menu OSD	angielski, japoński, niemiecki, francuski, rosyjski, portugalski, hiszpański
Cyfrowa redukcja szumu	2D-DNR, wł./wył.
Balans bieli	ATW, User1, User2, ANTI-CR, Manual, Push
Automatyczna regulacja wzmocnienia (AGC)	wł./wył.
Kompensacja tylnego oświetlenia	BLC, 3 poziomy/wył.
Redukcja migotania	wł./wył typowo 37dB, regulowana w zakresie od 6 dB do 44,80 dB
Strefy prywatne	4 programowalne strefy prywatne
Detekcja ruchu	4 programowalne strefy detekcji
Odbicie lustrzane obrazu	w poziomie
Elektroniczna migawka	1/50~1/120 000 sek.
Ręczna migawka	1/50 ~ 1/100 000 sek.
Zasilanie	12 V_{DC}
Pobór prądu	maks. 2 W/170 mA
Zakres temperatur /wilgotności pracy	-10°C~50°C/30%~80% RH
Masa	ok. 366 g

Monitor wideodomofonowy CDV-70P

COMMAX SmartHome & Security

Oferta firmy GDE Polska wzbogaciła się o nowy model monitora **COMMAX CDV-70P.** Monitor przeznaczony jest dla domów jedno- i wielorodzinnych oraz niewielkich budynków mieszkalnych. Ma 7-calowy ekran o wysokiej rozdzielczości z podświetleniem LED oraz sensoryczne przyciski służące do jego obsługi. Monitor może współpracować z dwoma panelami zewnętrznymi (obsługa dwóch wejść) lub z jednym panelem i dodatkową kamerą CCTV (podgląd większego obszaru). Wewnątrz lokalu możliwa jest rozbudowa systemu o dodatkowe monitory z serii CDV-xxx oraz unifony DP-4VHP wraz z obsługą funkcji interkomu. Monitor współpracuje z każdą kamerą COMMAX w systemie 4-żyłowym.

Charakterystyka

- Rodzaj ekranu: kolor LCD-LED
- Przekątna ekranu: 7"
- Rozdzielczość ekranu: 800×480 px
- Ilość obsługiwanych wejść: 2
- Funkcja interkomu: tak (monitor-monitor, monitor-unifon)
- Rodzaj monitora: głośnomówiący
- Standard sygnału wizyjnego: PAL/NTSC
- Funkcja otwierania bramy: opcja (poprzez moduł MD-RA-1)
- Regulacja głośności wywołania: tak
- Regulacja głośności rozmowy: tak
- Regulacja kontrastu: tak
- Regulacja jaskrawości obrazu: tak
- Zasilanie 230 V_{AC}
- Pobór mocy (praca / czuwanie): 15/3,5 VA
- Wymiary (szer.×wys.×gł.): 243×168×30 mm

Dystrybucja: GDE POLSKA

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany

tel./faks 12 256 50 35, 256 50 25
faks 12 270 56 96
e-mail: biuro@gde.pl

Depozytor na klucze systemowe SAIK LOCK

SAIK LOCK

Depozytor SAIK LOCK służy do bezpiecznego przechowywania, wydawania i przyjmowania kluczy. Każdy klucz znajdujący się w szafce jest chroniony i dostęp do niego mają tylko uprawnione osoby.

Klucze deponowane są w sposób uniemożliwiający podgląd ich profilów w trakcie przechowywania. W szafkach typu SAIK LOCK istnieje możliwość zastosowania systemów klucza generalnego dowolnego producenta. Jeśli funkcjonują one już w przedsiębiorstwie, nie ma potrzeby wymiany kluczy.

Wszystkie zdarzenia zachodzące w systemie są przez niego rejestrowane z uwzględnieniem daty, czasu oraz danych użytkownika i umożliwiają tworzenie szczegółowych raportów w oparciu o przyjęte kryteria.

Szafka SAIK LOCK wyposażona jest w duży ciekłokrystaliczny wyświetlacz z panelem dotykowym. Umożliwia to wygodne korzystanie z dodatkowych funkcji systemu - na przykład wbudowanej Rejestracji Czasu Pracy – czy wyświetlanie komunikatów od administratora.

Najważniejsze cechy

- Pobranie klucza tylko przez osoby upoważnione
- Zwrot klucza do dedykowanego otworu chroniącego profil klucza
- Wielkość depozytora dowolnie dostosowana do potrzeb klienta
- Duży, kolorowy wyświetlacz LCD z panelem dotykowym
- Standardowo montowany czytnik kart Mifare lub Unique
- Możliwość współpracy z dowolnym innym czytnikiem kart
- Możliwość współpracy z różnymi systemami kontroli dostępu, alarmowymi lub ppoż
- Wbudowane akumulatorowe zasilanie awaryjne
- Dołączone oprogramowanie instalowane na dowolnej ilości komputerów pozwalające na pełną kontrolę nad obiegiem kluczy w firmie
- Możliwość podglądu stanu szafki z poziomu przeglądarki internetowej
- Możliwość wyboru dowolnego koloru z palety RAL
- Możliwość dowolnej rozbudowy systemu
- Współpracuje z depozytorami wyposażonymi w tzw. breloki (typu SAIK KEY)
- Możliwość wbudowania kamery nadzorującej osoby korzystające z depozytora
- Podłączenie szafek do sieci LAN
- Wbudowana rejestracja czasu pracy (RCP)
- Możliwość dostosowania depozytora do potrzeb klienta

Producent:

bt electronics

bt electronics sp. z o.o.
Kraków, ul. Dukatów 10
31-431 Kraków

tel. 12 429 36 16, faks 12 410 85 11
e-mail: kontakt@saik.pl
www.saik.pl, www.bte.pl

SAIK SOFT – elektroniczny system wsparcia portiera

SAIK SOFT

System SAIK SOFT to rozwiązanie dla tych firm i instytucji, które potrzebują łatwo i kompleksowo usprawnić organizację obiegu kluczy używanych przez pracowników.

Osoby odpowiedzialne za wydawanie kluczy wyposażone są w elektroniczny Rejestrator Portiera SAIK SOFT. Za pomocą tego urządzenia każde wydanie i zwrot klucza jest odnotowywane przez dołączone oprogramowanie. Dzięki niemu zawsze istnieje możliwość kontroli nad tym kto, kiedy i jaki klucz pobrał.

Co równie istotne, pracownicy mogą dostać tylko ten klucz, do którego mają uprawnienia i tylko w godzinach określonych przez administratora. Takie rozwiązanie pozwala skrócić do niezbędnego minimum czas potrzebny na pobranie i zwrot klucza, zachowując jednocześnie obowiązujące standardy bezpieczeństwa.

System SAIK SOFT posiada także wbudowany moduł rejestracji czasu pracy (RCP), dzięki temu każde przyłożenie przez pracownika karty do czytnika może określać jego czas pracy. W ten sposób system SAIK SOFT można wykorzystywać dla wszystkich pracowników, lub tylko dla wydzielonej ich części.

Zastosowanie SAIK SOFT całkowicie eliminuje konieczność wypełniania i przechowywania dokumentów takich jak np. księga ewidencji kluczy, książka wejść-wyjść, zeszyt wyjść służbowych. Dzięki temu przewyższa te rozwiązania funkcjonalnością i ilością gromadzonych informacji.

Zaawansowane oprogramowanie, składające się z części administracyjnej, raportowej i alarmowej pozwala na dostosowanie systemu do indywidualnych potrzeb Klienta. Typ rejestratora, liczba obsługiwanych kluczy oraz inne elementy systemu mogą być dowolnie dopasowane do wymagań obiorcy.

Najważniejsze cechy

- Identyfikacja użytkowników w oparciu o osobiste karty zbliżeniowe
- Do każdego klucza przypięty jest brelok, na którym zaszyfrowane są informacje umożliwiające identyfikację klucza
- Każdy pracownik posiada przypisane do siebie klucze
- Elastycznie definiowane przedziały czasowe dostępu do kluczy
- Akumulatorowe zasilanie awaryjne Rejestratora Portiera
- Łatwa wymiana kluczy, możliwa do wykonania przez administratora
- Archiwizacja wszystkich zdarzeń zachodzących w systemie
- Wielostanowiskowe oprogramowanie systemowe pozwalające na przyjazne administrowanie systemem
- Gwarancja jakości i prawidłowej pracy systemu – produkt polski
- Stała 24 h obsługa techniczna
- Wbudowana rejestracja czasu pracy (RCP)

Producent:

bt electronics

bt electronics sp. z o.o.
Kraków, ul. Dukatów 10
31-431 Kraków

tel. 12 429 36 16, faks 12 410 85 11
e-mail: kontakt@saik.pl
www.saik.pl, www.bte.pl

AAT Holding sp. z o.o.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46
faks 22 546 05 01
e-mail: aat.warszawa@aat.pl
www.aat.pl

Oddziały:
ul. Koniczynowa 2A, 03-612 **Warszawa II**
tel./faks 22 743 10 11, 811 13 50
e-mail: aat.warszawa-praga@aat.pl

ul. Łęczycka 37, 85-737 **Bydgoszcz**
tel./faks 52 342 91 24, 342 98 82
e-mail: aat.bydgoszcz@aat.pl

ul. Ks. W. Siwka 17, 40-318 **Katowice**
tel./faks 32 351 48 30, 256 60 34
e-mail: aat.katowice@aat.pl

ul. Prosta 25, 25-371 **Kielce**
tel./faks 41 361 16 32/33
e-mail: aat.kielce@aat.pl

ul. Mieszczańska 18/1, 30-313 **Kraków**
tel./faks 12 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

ul. Energetyków 13a, 20-468 **Lublin**
tel. 81 744 93 65/66
faks 81 744 91 77
e-mail: aat.lublin@aat.pl

ul. Dowborczyków 25, 90-019 **Łódź**
tel./faks 42 674 25 33, 674 25 48
e-mail: aat.lodz@aat.pl

ul. Racławicka 82, 60-302 **Poznań**
tel./faks 61 662 06 60/62
e-mail: aat.poznan@aat.pl

Al. Niepodległości 659, 81-855 **Sopot**
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

ul. Zielona 42, 71-013 **Szczecin**
tel./faks 91 483 38 59, 489 47 24
e-mail: aat.szczecin@aat.pl

ul. Na Niskich Łąkach 26, 50-422 **Wrocław**
tel./faks 71 348 20 61, 348 42 36
e-mail: aat.wroclaw@aat.pl

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 22 832 47 44
faks 22 832 46 44
e-mail: biuro@acss.com.pl
www.acss.com.pl

AGIS Fire & Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. 22 430 83 01
faks 22 430 83 02
e-mail: agisfs.pl@agisfs.com
www.agisfs.pl

ALARM SYSTEM
ul. Kolumba 59
70-035 Szczecin
tel. 91 433 92 66
faks 91 489 38 42
e-mail: biuro@bonelli.com.pl
www.bonelli.com.pl

ALARMNET Sp. J.
ul. Karola Miarki 20c
01-496 Warszawa
tel. 22 663 40 85
faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl

ALARMTECH POLSKA Sp. z o.o.
Oddział:
ul. Kielnieńska 115
80-299 **Gdańsk**
tel. 58 340 24 40
faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

ALKAM SYSTEM Sp. z o.o.
ul. Bydgoska 10
59-220 Legnica
tel. 76 862 34 17, 862 34 19
faks 76 862 02 38
e-mail: alkam@alkam.pl
www.alkam.pl

ALPOL Sp. z o.o.
ul. Ścigały 10
40-208 Katowice
tel. 32 790 76 16
faks 32 790 76 60
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

Oddziały:
ul. Warszawska 56, 43-300 **Bielsko-Biała**
tel. 32 790 76 21
faks 32 790 76 64
e-mail: bielsko@e-alpol.com.pl

ul. Łęczycka 55, 85-737 **Bydgoszcz**
tel. 32 720 39 65
faks 32 790 76 85
e-mail: bydgoszcz@e-alpol.com.pl

ul. Uszczyka 11, 44-100 **Gliwice**
tel. 32 790 76 23
faks 32 790 76 65
e-mail: gliwice@e-alpol.com.pl

ul. Paulinów 10, 67-200 **Głogów**
tel. 32 750 30 78
faks 32 750 30 69
e-mail: glogow@e-alpol.com.pl

ul. Sandomierska 105, 25-324 **Kielce**
tel. 32 720 39 82
faks 32 790 76 94
e-mail: kielce@e-alpol.com.pl

ul. Pachońskiego 2a, 31-223 **Kraków**
tel. 32 790 76 46
faks 32 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Nowodworska 23, 59-200 **Legnica**
tel. 32 750 30 66
faks 32 750 30 67
e-mail: legnica@e-alpol.com.pl

ul. Grenadierów 13, 20-331 **Lublin**
tel. 32 790 76 50
faks 32 790 76 74
e-mail: lublin@e-alpol.com.pl

ul. Senatorska 31, 93-192 **Łódź**
tel. 32 790 76 25
faks 32 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. T. Kutrzeby 16G/112, 61-719 **Poznań**
tel. 32 790 76 37
faks 61 826 63 36
e-mail: poznan@e-alpol.com.pl

ul. Młodzianowska 75d, 26-600 **Radom**
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@e-alpol.com.pl

ul. Rzemieślnicza 13, 81-855 **Sopot**
tel. 32 790 76 43
faks 32 790 76 72
e-mail: sopot@e-alpol.com.pl

ul. Dąbrowskiego 25, 70-100 **Szczecin**
tel. 32 790 76 30
faks 32 790 76 68
e-mail: szczecin@e-alpol.com.pl

ul. Polna 134/136, 87-100 **Toruń**
tel. 32 750 30 80
faks 32 750 30 73
e-mail: torun@e-alpol.com.pl

ul. Rzymowskiego 34, 02-697 **Warszawa-Mokotów**
tel. 32 790 76 34
faks 32 790 76 69
e-mail: warszawa@e-alpol.com.pl

ul. Floriana 3/5, 04-664 **Warszawa-Praga**
tel. 32 790 76 33
faks 32 790 76 71
e-mail: warszawa2@e-alpol.com.pl

ul. Spółdzielcza 3, 87-800 **Włocławek**
tel. 32 750 30 43
faks 32 750 30 45
e-mail: wloclawek@e-alpol.com.pl

ul. Stargardzka 7-9, 54-156 **Wrocław**
tel. 32 790 76 27
faks 32 790 76 67
e-mail: wroclaw@e-alpol.com.pl

ul. Dekoracyjna 3, 65-722 **Zielona Góra**
tel. 32 750 30 70
faks 32 750 30 71
e-mail: zielona@e-alpol.com.pl

ASSA ABLOY

ASSA ABLOY POLAND Sp. z o.o.
ul. Jana Olbrachta 94
01-102 Warszawa
tel. 22 751 53 54
faks 22 751 53 56
e-mail: biuro@assaabloy.com.pl
www.assaabloy.com.pl

FIRMA ATLine Sp. J.
ul. Franciszkańska 125
91-845 Łódź
tel. 42 23 13 849÷851, 42 23 63 019
faks 42 655 20 99
e-mail: handel@atline.pl
www.atline.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 41 00
faks 22 715 41 05
e-mail: dominika.kolodziejska@pl.bosch.com
www.boschsecurity.pl

P.W.H. BRABORK-LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
tel. 22 619 29 49
faks 22 619 25 14
e-mail: brabork@braborklab.pl
www.braborklab.pl

bt electronics sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. 12 410 85 10
faks 12 410 85 11
e-mail: saik@saik.pl
www.saik.pl

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
Tulipan Hause
02-672 Warszawa
Infolinia 801 133 084
faks 22 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
86-050 Solec Kujawski
tel. 52 387 36 58
faks 52 387 54 66 wew. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

CBC (POLAND) Sp. z o.o.
ul. Krasińskiego 41A
01-755 Warszawa
tel. 22 633 90 90
faks 22 633 90 60
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

CMA MONITORING
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888
faks 22 546 0 619
e-mail: info@cma.com.pl
www.cma.com.pl

Oddziały:
ul. Świętochłowicka 3, 41-909 **Bytom**
tel. 32 388 0 950
faks 32 388 0 960
e-mail: bytom@cma.com.pl

ul. Zatorska 36, 51-215 **Wrocław**
tel. 71 340 0 209
faks 71 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. 12 260 13 96
tel. kom. 665 380 677
faks 12 260 13 95

ul. Palacza 127, 60-279 **Poznań**
tel./faks 61 861 40 51
tel. kom. 601 203 664
e-mail: poznan@cma.com.pl

Al. Niepodległości 659, 81-855 **Sopot**
tel. 58 345 23 24
tel. kom. 693 694 339
e-mail: sopot@cma.com.pl

D-MAX Polska Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel./faks 61 822 60 52
e-mail: dmax@dmaxpolska.pl
www.dmaxpolska.pl

DG ELPRO Sp. J.
ul. Wadowicka 6
30-415 Kraków
tel. 12 263 93 85
faks 12 263 93 86
e-mail: biuro@dgelpro.pl
www.dgelpro.pl

DYSKAM-EKOTRADE Sp. z o.o.
ul. Reymonta 22
30-059 Kraków
tel. 12 637 80 20
faks 12 637 80 20 wew. 23
e-mail: dyskam@dyskam.com.pl
www.dyskam.com.pl

DYSKRET POLSKA
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Mazowiecka 131
30-023 Kraków
tel. 12 423 31 00
faks 12 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 812 05 05
faks 22 812 62 12
e-mail: sales@ebs.pl
www.ebs.pl

Ela-compil sp. z o.o.
ul. Słoneczna 15A
60-286 Poznań
tel. 61 869 38 50
faks 61 861 47 40
e-mail: office@ela.pl
www.ela-compil.pl

EL-MONT
ul. Wyzwolenia 15
44-200 Rybnik
tel. 32 423 07 28, 422 38 89
faks 32 423 07 29
e-mail: el-mont@el-mont.com
www.el-mont.com

PHU ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel. 22 398 96 53
faks 22 398 96 54
e-mail: elproma@elproma.pl
www.elproma.pl

EUREKA SOFT & HARDWARE
ul. Rynek 13
62-300 Września
tel. 61 437 90 15
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

FACTOR SECURITY Sp. z o.o.
ul. Garbary 14B
61-867 Poznań
tel. 61 850 08 00
faks 61 850 08 04
e-mail: factor@factor.pl
www.factor.pl

Oddział:
ul. Morelowa 11A, 65-434 **Zielona Góra**
tel. 68 452 03 00
tel./faks 68 452 03 01
e-mail: factor.zg@factor.pl

FES Trading Sp. z o.o.
ul. Schuberta 100
80-171 Gdańsk
tel. 58 340 00 41 ÷ 44
faks 58 340 00 45
e-mail: fes@fes.pl
www.fes.pl

GDE POLSKA
Leszek Mitusiński
ul. Świątnicka 88
Włosań
32-031 Mogilany
tel. 12 256 50 35
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

GEO-KAT Sp. z o.o.
ul. Taneczna 7
02-829 Warszawa
tel. 22 877 08 80
faks 22 877 08 97
e-mail: info@geokat.com.pl
www.geokat.com.pl

ICS POLSKA
ul. Poleczki 82
02-822 Warszawa
tel. 22 646 11 38
faks 22 849 94 83
e-mail: biuro@ics.pl
www.ics.pl

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 98 44, 411 57 47
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 2
02-490 Warszawa
tel. 22 863 63 53
faks 22 863 74 23
e-mail: janex@janexint.com.pl
www.janexint.com.pl

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. 32 324 89 00
faks 32 324 89 01
e-mail: firma@kabe.pl
www.kabe.pl

KATON Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa
tel. 22 869 43 92
faks 22 869 43 93
e-mail: biuro@katon.eu
www.katon.eu

KOLEKTOR
K. Mikiciuk i R. Rutkowski Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel./faks 58 553 67 59
e-mail: info@kolektor.pl
www.kolektor.pl

MICROMADE
Gałka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
www.micromade.pl

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
faks wew. 28
e-mail: info@micronix.pl
www.micronix.pl

NOVATEL Sp. z o.o.
ul. Turystyczna 1
43-155 Bieruń
tel. 32 201 17 04
faks 32 201 15 11
e-mail: novatel@novatel.pl
www.novatel.pl

NUUXE – RADIOTON Sp. z o.o.
ul. Olszańska 5
31-513 Kraków
tel. 12 393 58 00
faks 12 393 58 02
e-mail: cctv@jvcpro.pl
www.jvcpro.pl
www.nuuxe.com

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel./faks 71 343 16 76
e-mail: obis@obis.com.pl
www.obis.com.pl

OMC INDUSTRIAL Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. 22 651 88 61
faks 22 651 88 76
e-mail: sprzedaz@omc.com.pl
www.omc.com.pl

Przedstawicielstwo:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks 32 202 55 82
e-mail: katowice@omc.com.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks 61 657 93 60
e-mail: poznan@omc.com.pl

ul. Różyckiego 1c, 51-608 **Wrocław**
tel./faks 71 347 91 91
e-mail: wroclaw@omc.com.pl

POINTEL Sp. z o.o.
ul. Fordońska 199
85-739 Bydgoszcz
tel. 52 371 81 16
faks 52 342 35 83
e-mail: biuro@pointel.pl
www.pointel.pl

POL-ITAL Sp. z o.o.
ul. Irysowa 11
02-660 Warszawa
tel. 22 831 15 35
faks 22 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

POLON-ALFA
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61
faks 52 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. 61 842 29 62
faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl

PULSAR K. Bogusz Sp. J.
Siedlec 150
32-744 Łapczyca
tel. 14 610 19 40
faks 14 610 19 50
e-mail: norbert@pulsar.pl
www.pulsar.pl

RAMAR s.c.
ul. Modlińska 237
03-120 Warszawa
tel./faks 22 676 77 37, 676 82 87
faks 22 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

RETT-POL
Bogusław Godlewski
ul. Podmiejska 21
01-498 Warszawa
tel. 22 632 72 22
faks 22 833 09 07
e-mail: biuro@rettpol.pl
www.rettpol.pl

RISCO GROUP POLAND Sp. z o.o.
ul. 17 Stycznia 56
02-146 Warszawa
tel. 22 500 28 40
faks 22 500 28 41
e-mail: sales-pl@riscogroup.com
www.riscogroup.com

ROPAM Elektronik s.c.
Os. Tysiąclecia 6A/1
32-400 Myślenice
tel. 12 341 04 07
faks 12 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.pl
www.ropam.eu

SAMSUNG TECHWIN EUROPE LIMITED
Biuro w Polsce
ul. Postępu 15c
02-676 Warszawa
tel. 22 20 50 777
faks 22 20 50 763
e-mail: STEsecurity@samsung.com
www.samsungsecurity.com

SATEL Sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
tel. 58 320 94 00
faks 58 320 94 01
e-mail: satel@satel.pl
www.satel.pl

SAWEL
Systemy Bezpieczeństwa
ul. Lwowska 83
35-301 Rzeszów
tel./faks 17 857 80 60
e-mail: sawel@sawel.com.pl
www.sawel.com.pl

SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. Iłżecka 24
02-135 Warszawa
tel. 22 313 24 15, 511 84 64
faks 22 313 24 10
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.com

Oddziały:
ul. Arkońska 6 bud. A2
80-387 **Gdańsk**
tel. 58 782 00 01
faks 58 782 00 04

ul. Muchoborska 18
54-424 **Wrocław**
tel. 71 711 09 19
faks 71 711 09 20

ul. Krakowska 280
32-080 **Zabierzów k. Krakowa**
tel. 12 257 60 80
faks 12 257 60 81

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44a
02-672 Warszawa
tel. 22 33 00 620÷623
faks 22 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
CH Manhattan, III piętro
Al. Grunwaldzka 82, 80-244 **Gdańsk**
tel./faks 58 767 70 10
e-mail: gdansk@schrack-seconet.pl

ul. Wierzbięcice 1, 61-569 **Poznań**
tel. 61 833 31 53
faks 61 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-520 **Wrocław**
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

P.T.H. SECURAL
Jacek Giersz
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. 32 291 86 17
faks 32 291 88 10
e-mail: info@secural.com.pl
www.secural.com.pl

SMA Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. 22 651 88 61
faks 22 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

Oddziały:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks 32 202 55 82
e-mail: katowice@sma.biz.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks 61 657 93 60
e-mail: poznan@sma.biz.pl

ul. Różyckiego 1C, 51-608 **Wrocław**
tel. 71 347 91 91
tel./faks 71 348 04 19
e-mail: sma@sma.wroclaw.pl

SPS Electronics Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spselectronics.pl
www.spselectronics.pl

Biura Handlowe:
ul. Drożyny 6, 80-302 **Gdańsk**
tel. 58 624 83 04
faks 58 668 59 20
e-mail: gdansk@spselectronics.pl

ul. Kościuszki 227, 40-600 **Katowice**
tel. 32 255 64 27
faks 32 255 64 52
e-mail: katowice@spselectronics.pl

ul. Drewnowska 48, 91-002 **Łódź**
tel. 42 617 00 32
faks 42 659 85 23
e-mail: lodz@spselectronics.pl

ul. Polska 60, 60-595 **Poznań**
tel. 61 852 19 02
faks 61 825 09 03
e-mail: poznan@spselectronics.pl

ul. Grudziądzka 176, 87-100 **Toruń**
tel. 56 653 99 43
faks 56 653 90 81
e-mail: torun@spselectronics.pl

pl. Gen. Wróblewskiego 3a, 50-413 **Wrocław**
tel. 71 348 44 64
faks 71 348 36 35
e-mail: wroclaw@spselectronics.pl

SECURITY SOLUTION NETWORK Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. 61 842 29 62
faks 61 842 29 62
e-mail: ssn@ssn.net.pl
www.ssn.net.pl

TAP- Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. 22 843 83 95
faks 22 843 79 12
e-mail: tap5@tap.com.pl

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. 22 516 97 97
faks 22 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

UNICARD S.A.
ul. Łagiewnicka 54
30-417 Kraków
tel. 12 398 99 18
faks 12 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. 52 345 45 00
faks 52 584 01 92
e-mail: biuro@w2.com.pl
www.w2.com.pl

VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. 61 623 23 05
faks 61 623 23 17
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

ZBAR PHU
Mariusz Popenda
ul. Krakowska 60
94-214 Łódź
tel. 42 611 12 98
faks 42 611 12 97
e-mail: zbar@zbar.com.pl
www.zbar.com.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS Fire & Security	–	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	TAK	–	–
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	–	TAK	–	TAK
ASSA ABLOY	–	–	TAK	–	TAK
FIRMA ATLine	–	TAK	TAK	TAK	–
BOSCH	TAK	–	–	–	–
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	–	TAK	–	–
CBC (Poland)	TAK	TAK	TAK	–	TAK
CMA	TAK	–	–	TAK	–
D-MAX	–	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
Ela-compil	TAK	–	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
GEO-KAT	–	TAK	TAK	TAK	–
ICS POLSKA	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
Janex International	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Kolektor	–	TAK	TAK	TAK	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
Novatel	TAK	TAK	TAK	TAK	TAK
Nuuxe – Radioton	–	TAK	TAK	TAK	TAK
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	–	TAK	–	–
Pulsar	TAK	–	–	–	–
Ramar	–	TAK	TAK	TAK	TAK
RETT-POL	–	TAK	TAK	TAK	TAK
RISCO	TAK	–	–	–	–
ROPAM Elektronik	TAK	–	TAK	–	TAK
Samsung	TAK	–	TAK	–	–
Satel	TAK	TAK	–	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	TAK	–	TAK	–	–
Schrack Seconet Polska	TAK	TAK	TAK	–	TAK
Secural	TAK	TAK	TAK	–	TAK
SMA	–	TAK	–	TAK	–
SPS Electronics	–	TAK	TAK	–	TAK
SSN	–	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Technokabel	TAK	–	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	TAK	TAK	–	TAK
ZBAR	–	TAK	TAK	TAK	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
AGIS Fire & Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	TAK	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
FIRMA ATLine	TAK	–	TAK	–	TAK	TAK	–	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC (Poland)	–	TAK	–	–	–	–	–	–	–
CMA	TAK	TAK	–	–	–	TAK	TAK	–	–
D-MAX	–	TAK	–	–	–	–	–	–	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Dyskam-Ekotrade	TAK	TAK	–	TAK	–	–	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	Transmitery IP/GSM/GPRS, systemy RFID, zabezpieczenia energetyka, bankowość, produkcja OEM/ODM								
Ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	TAK
FES	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	–	TAK	–
GEO-KAT	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
ICS POLSKA	TAK	TAK	TAK	TAK	TAK	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Janex International	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Novatel	–	–	–	–	–	TAK	–	–	TAK
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	TAK
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	–	–	–	TAK	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RETT-POL	TAK	TAK	TAK	TAK	–	–	–	–	–
RISCO	TAK	–	TAK	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	–	–	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
SMA	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SPS Electronics	TAK	TAK	TAK	TAK	–	–	TAK	–	–
SSN	–	TAK	TAK	–	–	–	–	–	–
Tap – Systemy Alarmowe	TAK	TAK	TAK	–	–	TAK	–	–	–
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
UNICARD	TAK	TAK	TAK	TAK	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	TAK	–	–	–
ZBAR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Paweł Karczmarzyk
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner
Andrzej Wójcik

Skład i łamanie
Tomasz Kaczmarczyk

Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. 22 546 0 951, 953
faks 22 546 0 959
www.zabezpieczenia.com.pl

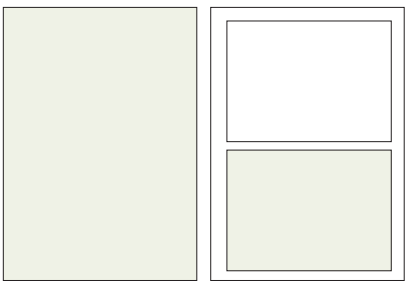
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4200 zł
cała strona, czarno-biała	2200 zł
1/2 strony, pełny kolor	2700 zł
1/2 strony, czarno-biała	1500 zł
1/3 strony, pełny kolor	1900 zł
1/3 strony, czarno-biała	1000 zł
1/4 strony, pełny kolor	1400 zł
1/4 strony, czarno-biała	800 zł
karta katalogowa, 1 strona	900 zł



cała strona (200 x 282 mm + 3mm spad)

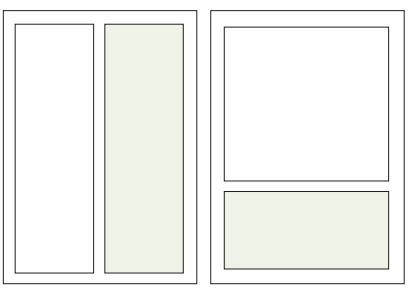
1/2 strony (170 x 125 mm)

Artykuł sponsorowany:

Cena za stronę artykułu sponsorowanego w czasopiśmie to 1500 zł (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



1/2 strony (83 x 260 mm)

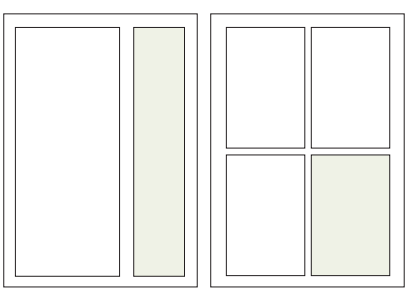
1/3 strony (170 x 80 mm)

Spis teleadresowy:

jednorazowy wpis	70 zł

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej **http://www.zabezpieczenia.com.pl** w dziale **Reklama**

Spis reklam

OCHRONA OBWODOWA OBIEKTÓW CCTV

ZBAR

_ CCTV

- kamery laserowe
- kamery termowizyjne
- hybrydowe kamery termowizyjne w technologii laserowej
- systemy transmisji światłowodowej
- rejestratory: DVR, NVR, hybrydowe (DVR/NVR), mobilne DVR
- kamery IP i analogowe
- systemy ścian wideo „video wall"

_ Intelligent Video Analytic
Inteligentna Analiza Obrazu

- tworzenie wirtualnego ogrodzenia
- zliczanie ludzi/pojazdów
- detekcja zniknięcia/pojawienia się obiektu
- klasyfikacja obiektów
- detekcja sabotażu kamery
- rozbudowana detekcja ruchu
- filtr prędkości obiektu

94-214 Łódź, Poland, Krakowska 60
Tel. + 48 **426 111 298**, Fax +48 **426 111 297**
e-mail: zbar@zbar.com.pl

sprawdź pełną ofertę na **www.zbar.com.pl**

Aventura · FFT · PFOtech · CIAS · SCHRACK SECONET · SENSTAR · GPS · IFTER

Platforma wymiany informacji

HID iCLASS SE

Otwarta, elastyczna i doskonale zabezpieczona platforma iCLASS SE®, która ułatwia wszystko.

HID®

iCLASS SE® to kolejna generacja platformy kontroli dostępu HID Global, która umożliwia uwierzytelnianie w różnych komercyjnych technologiach przy użyciu kart bezkontaktowych. Bardzo elastyczna rodzina czytników wraz z szeroką gamą kart zbliżeniowych zapewnia wymianę informacji w różnych środowiskach technologicznych. Technologia iCLASS SE może zostać również użyta w telefonach komórkowych (NFC) i innych urządzeniach inteligentnych. Teraz możesz wykorzystać wszystkie możliwości tej technologii do stworzenia idealnego systemu kontroli dostępu. **Aby uzyskać więcej informacji, odwiedź hidglobal.com/path-Zab**