CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(65)/2009

ZABEZPIECZENIA

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

W NUMERZE:

Professional Series

Czujki ruchu, które potrafią odróżnić prawdziwe zagrożenie od źródeł fałszywych alarmów

Rewolucyjna technologia przetwarzania danych z kilku detektorów to prawdziwy przełom w inteligentnym wykrywaniu zagrożeń.

BOSCH
Technologia bliżej nas

- Wyjątkowa skuteczność wykrywania i eliminacja fałszywych alarmów
- Dostępna jedynie w rozwiązaniach firmy Bosch technologia wspólnego przetwarzania sygnałów z pięciu detektorów
- Najwyższa skuteczność detekcji dzięki ciągłemu dostosowywaniu czułości detektorów
- Funkcja aktywnej redukcji białego światła oraz trójogniskowy układ optyczny eliminują fałszywe alarmy, zapewniając najlepszą skuteczność wykrywania we wszystkich zasięgach
- Teraz z technologią wielopunktowego antymaskingu i zintegrowanym wykrywaniem zablokowania soczewki sprayem
- Możliwość dostosowania wszystkich modeli do każdego zastosowania

Aby uzyskac więcej informacji, zapraszamy do odwiedzenia naszej strony internetowej www.boschsecurity.pl

Robert Bosch Sp. z o.o.
Security Systems
ul. Poleczki 3, 02-822 Warszawa
tel.: +48 22 715 41 00 / 01, fax: +48 22 715 41 05 / 06
securitysystems@pl.bosch.com **www.boschsecurity.pl**

Spis treści

CZASOPISMO ZABEZPIECZENIA 1/2009

Easy Rider 23

Kamery AutoDome i oświetlenie podczerwienią 35

Profesjonalizm w zarządzaniu bezpieczeństwem firmy 47

Biometria z NOVUSA (część I) 62

Panasonic i SANYO zawierają przymierze

19 grudnia 2008 roku firmy **Panasonic Corporation** i **SANYO Electric Co.** ogłosiły, że zawierają przymierze kapitałowe i biznesowe, w wyniku którego w obu firmach przewidziane są zmiany organizacyjne i strukturalne. Marka Panasonic była znana z innowacyjnego myślenia oraz z dostarczania przyszłościowych „pomysłów na życie". Z drugiej strony widoczne było dążenie SANYO do stania się czołową firmą w zakresie wykorzystania energii i ochrony środowiska. Firmy Panasonic i SANYO, działając wspólnie, chcą podnosić jakość życia na całym świecie oraz działać w harmonii ze środowiskiem. Stanie się to możliwe dzięki połączeniu posiadanych i stosowanych technologii i wiedzy produkcyjnej obu firm. Główne obszary, w których oczekuje się wystąpienia efektu synergicznego, to:

– wykorzystanie energii słonecznej, m.in. przez intensyfikację rozwoju i komercjalizacji ogniw słonecznych następnej generacji;
– rozwój źródeł energii mobilnej, tj. akumulatorów, głównie dla pojazdów o napędzie hybrydowym (HEV – ang. *Hybrid Electric Vehicle*) i elektrycznym (EV – ang. *Electric Vehicle*);
– umocnienie pozycji finansowej i biznesowej, m.in. dzięki spodziewanej obniżce kosztów zakupu materiałów oraz kosztów związanych z logistyką.

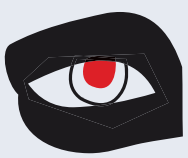
Zgodnie z zawartym porozumieniem Panasonic i SANYO utworzą komitet ds. współpracy, który zajmie się takimi sprawami, jak systemy zarządzania, rozwój technologii, zaopatrzenie i logistyka, kontrola jakości oraz infrastruktura informatyczna, w celu jak najszybszego uzyskania efektów współpracy po tym, jak SANYO stanie się filią firmy Panasonic.

Panasonic Corporation jest światowym liderem w rozwijaniu i wytwarzaniu produktów elektronicznych do zastosowań powszechnego użytku, biznesowych i przemysłowych (więcej informacji na http://panasonic.net).

SANYO Electric Co. działa w trzech obszarach biznesowych: energia, elektronika i ekologia, oferując szeroki asortyment produktów i usług, takich jak akumulatory, systemy fotowoltaiczne, urządzenia do ogrzewania, wentylacji, klimatyzacji i chłodnictwa, systemy do obrazowania cyfrowego, urządzenia do nawigacji osobistej, artykuły gospodarstwa domowego, komponenty elektroniczne i inne (więcej informacji na http://www.sanyo.com).

Bezpośr. inf. Panasonic UK
Opracowanie: Adam Bułaciński, Redakcja

Ośrodek Szkoleniowy Polskiej Izby Systemów Alarmowych zaprasza na kursy i seminaria:



– kurs pracownika zabezpieczenia technicznego pierwszego stopnia „Instalowanie i konserwacja systemów zabezpieczeń technicznych Klas SA1–SA4",
– kurs pracownika zabezpieczenia technicznego drugiego stopnia „Projektowanie systemów zabezpieczeń technicznych klas SA1–SA4",
– kurs inwestorów systemów zabezpieczeń technicznych,
– kurs pracownika zabezpieczenia technicznego „Montaż, eksploatacja, konserwacja i naprawa urządzeń i środków mechanicznego zabezpieczenia",
– kurs kosztorysowania systemów zabezpieczeń technicznych,
– kurs ekspertów i doradców w zakresie bezpieczeństwa,
– kursy specjalistyczne,
– seminarium projektowe,
– seminarium instalacyjne.

Seminaria adresowane są do osób, które ukończyły stosowne kursy w innych ośrodkach szkoleniowych.

Absolwenci kursów i seminariów otrzymują dwa dokumenty wystawione bezterminowo:

– zaświadczenie o ukończeniu kursu (druk MEN),
– dyplom OS PISA.

Z pełną ofertą szkoleniową Ośrodka Szkoleniowego PISA można zapoznać się na stronie *www.pisa.org.pl*.

Szczegółowe informacje można uzyskać w OS PISA (tel.: 022 620 45 57, e-mail: ospisa@pisa.org.pl).

Bezpośr. inf. Roma Kostrzewa
OS PISA

Współpraca Sony z Wyższą Szkołą Menedżerską

Firma **Sony** rozpoczęła współpracę z **Wyższą Szkołą Menedżerską** (Warszawa, ul. Kawęczyńska). Uczelnia kształci na studiach licencjackich i inżynierskich oraz prowadzi zarówno studia pięcioletnie, jak i uzupełniające studia magisterskie. Firma Sony wyposażyła **Laboratorium Systemów Alarmowych** w sprzęt IPELA, czyli kamery sieciowe IP, kamery analogowe, wideoserwery oraz oprogramowanie Real Shot Manager. Sala ćwiczeń została przygotowana tak, by można było poznać budowę sieci IP i możliwości, jakie niesie ze sobą ta technologia. Udostępniono również kamery analogowe i wideoserwery, dzięki którym można stworzyć system hybrydowy. Wszystkie kamery pracują w systemie Real Shot Manager, pozwalającym na tak zaawansowane funkcje, jak detekcja ruchu czy detekcja obiektów. Absolwenci kierunku bezpieczeństwo obiektów i informacji będą specjalistami w swojej dziedzinie dzięki temu, że już na wczesnym etapie nauki będą mieli kontakt z kluczowym dostawcą technologii, jakim jest firma Sony.

Bezpośr. inf. Marta Małecka
Sony Poland

Maksimum bezpieczeństwa, minimum zużycia pasma

Firma **Sony** była pierwszym producentem na rynku kamer IP CCTV, który wprowadził kodowanie obrazu w formacie H.264. Seria kodeków MPEG-4 jest zgodna ze standardami ISO/IEC, w odróżnieniu od innych formatów wykorzystywanych czasem przez obecnych na rynku telewizji dozorowej producentów, i należy do rodziny kodeków MPEG: Motion Pictures Experts Group. MPEG-4 w wersji 2 jest wykorzystywany przez prawie wszystkie kamery Sony. W roku 2006 Sony wprowadziło do kamer IP CCTV kolejną generację MPEG-4, mianowicie kodek H.264 (czyli MPEG-4 w wersji 10). Kodek ten został stworzony w celu poprawienia jakości obrazu wideo przy zużyciu mniejszego pasma przesyłu niż MPEG-4. Firma Sony wykorzystuje H.264 zarówno w produktach profesjonalnych (wideokonferencje i kamery IP CCTV), jak i konsumenckich (PSP, Blu-ray) już od roku 2005.

Wykorzystanie kodeka H.264 daje zupełnie nowe możliwości przesyłu obrazu wideo: dużo lepszą jakość, mniejsze zużycie pasma, oszczędność powierzchni dyskowych. Dla porównania: MPEG-4 zajmuje około jednej trzeciej pasma zajmowanego przez JPEG, a H.264 około jednej piątej. Sony ma w swojej ofercie osiem różnych modeli kamer, które umożliwiają wykorzystanie kodeka H.264. Są to: stałopozycyjna kamera SNC-CS50P, kopułowe kamery SNC-DF50P, SNC-DF80P i SNC-DF85P oraz kamery Pan-Tilt-Zoom SNC-RZ50, SNC-RX530P, SNC-RX550P oraz SNC-RX570P.

Wykorzystanie tego kodeka do transmisji obrazów ruchomych okazało się dużym krokiem do przodu. Potwierdza to również fakt, że pozostałe firmy powoli wprowadzają ten format kodowania do swojej oferty.

Wykorzystując nowoczesne technologie, można radykalnie zwiększyć elastyczność i wydajność systemu IP. Trzeba jednak pamiętać, że większa kompresja oznacza większe wymagania odnośnie procesora, po którego stronie jest dokonywane dekodowanie informacji.

Bezpośr. inf. Marta Małecka
Sony Poland

SG3 w sprzedaży

SG3ECO – pierwszy przedstawiciel zapowiadanej nowej linii produktów **SEVEN GUARD** jest dostępny w sprzedaży. Producent, firma SYSTEM 7 z Bielska-Białej, właśnie wprowadza – najpierw na krajowy rynek – pierwszą pilotażową partię tych ciekawych urządzeń.

SG3ECO przeszedł pomyślnie przez wielomiesięczną procedurę testowania i został dopuszczony do normalnej sprzedaży. Rejestratory z serii 3 są jeszcze bardziej wytrzymałe od swoich znanych od dziesięciu lat poprzedników. Ponadto do ich wykonania wykorzystano najnowsze dostępne rozwiązania technologiczne, np.: akumulatory polimerowe, hermetyczne, bardzo odporne obudowy stalowo-kompozytowe o grubości 5 mm oraz innowacyjne w skali świata rozwiązania techniczne.

Wszystkie urządzenia z nowej rodziny SG3 mogą zostać podłączone do komputera przez łącze USB lub RS232. Dodatkowym atutem rejestratora SG3ECO jest bardzo atrakcyjna cena.

Bezpośr. inf. SYSTEM 7

OŚWIADCZENIE

Zarządu Polskiej Izby Systemów Alarmowych

z 2 grudnia 2008 r.

1 maja 2004 roku na mocy Traktatu Ateńskiego Polska stała się członkiem Unii Europejskiej. Jednym z warunków wstępnych członkostwa Polski w Unii Europejskiej było uzyskanie przez Polski Komitet Normalizacyjny członkostwa w europejskich organizacjach normalizacyjnych. Warunkiem do spełnienia przez Polskę w procesie akcesyjnym była także harmonizacja polskiego systemu norm technicznych.

Pięć miesięcy przed akcesją Polski do UE Polski Komitet Normalizacyjny został członkiem europejskich organizacji normalizacyjnych, a tym samym uzyskał prawo uczestnictwa w opracowywaniu norm europejskich na równych prawach z jednostkami normalizacyjnymi innych krajów UE.

W wyniku powszechnego zainteresowania normami zharmonizowanymi z dyrektywami UE, które dotyczą m.in. bezpieczeństwa, ochrony zdrowia i życia, niezbędne stało się wzmożenie przez PKN prac związanych z tłumaczeniem i wprowadzeniem w Rzeczpospolitej Polskiej norm europejskich, wprowadzonych wcześniej metodą uznania (tj. przyjętych w oryginalnej wersji językowej). Plany i programy prac normalizacyjnych, opracowywane w kolejnych latach przez PKN, potwierdzają znaczenie tego zadania.

Od kilku lat branża zabezpieczeń technicznych obserwuje ten proces i oczekuje na wprowadzenie interesujących ją norm europejskich w języku polskim, po przetłumaczeniu ich z oryginału. Ustawa o normalizacji nie pozwala bowiem na powoływanie polskich norm w przepisach prawnych bez opublikowania ich w języku polskim.

Od kilku lat toczy się (m.in. na łamach prasy branżowej) publiczna dyskusja dowodząca archaiczności polskich norm dla systemów alarmowych.

W 2002 roku Polski Komitet Normalizacyjny przyjął w trybie uznania – w języku angielskim – normę europejską dotyczącą systemów alarmowych, nadając jej nazwę PN-EN-50131-1:2002(U).

Norma ta od lat pozostaje przedmiotem prac Komitetu Technicznego nr 52 PKN, podobnie jak dwie inne normy z tej serii, dawno już przetłumaczone na język polski. Przetłumaczone normy do dziś nie mogą stać się normami w j. polskim, mają w dalszym ciągu status norm przyjętych w Polsce metodą uznaniową i nie mogą tym samym zastąpić norm przestarzałych. Nie pozostaje to bez wpływu na przebieg procesu legislacyjnego związanego z nowelizacją ustawy o ochronie osób i mienia.

Od ponad dwóch lat przedstawiciele Komitetu Technicznego nr 52 PKN, którego Sekretariat prowadzi Stowarzyszenie „Polalarm", co jakiś czas ogłaszają, że normy cieszące się największym zainteresowaniem ze strony użytkowników będą sukcesywnie ustanawiane w polskiej wersji językowej.

Interesujące naszą branżę normy europejskie, w przeciwieństwie do dotychczas stosowanych w kraju, stawiają z pewnością wyższe wymagania dla najwyższych klas systemów zabezpieczeń technicznych. Są też w nich bardziej precyzyjne wymagania dla urządzeń w danych klasach. Dają ponadto użytkownikowi przejrzyste kryteria oceny, miernik jakości, gwarancję kompatybilności i współdziałania, a ich stosowanie stanowi gwarancję jakości produktu, na którym mogą polegać instalatorzy, dystrybutorzy i użytkownicy.

W świetle wyżej przedstawionej sytuacji Zarząd Polskiej Izby Systemów Alarmowych, mając na uwadze podstawowe cele normalizacji, jakimi są m.in. zapewnienie dostępu do nowoczesnych rozwiązań, usuwanie barier technicznych i tworzenie warunków skutecznej konkurencji, a przede wszystkim kierując się interesem prężnych przedsiębiorstw naszej branży, żywotnie zainteresowanych wprowadzeniem norm europejskich i uzyskaniem powyższych możliwości, oświadcza, że:

- pokryje koszty tłumaczenia dwóch norm będących już przedmiotem prac normalizacyjnych Komitetu Technicznego nr 52,
- pokryje koszty tłumaczenia kolejnych czterech najważniejszych dla branży norm europejskich, uznając, że problem braku środków finansowych stanowi jedyną przeszkodę na drodze do wprowadzenia norm europejskich do polskiej techniki zabezpieczeń,
- wyraża gotowość wykonania i sfinansowania tego zadania w trybie pilnym.

Zarząd PISA, doceniając dotychczasowe zaangażowanie i wyniki wieloletnich prac Komitetu Technicznego 52, oczekuje od Komitetu wykazania zainteresowania inicjatywą i deklaracją PISA oraz podjęcia równie pilnych prac normalizacyjnych w przyporządkowanym mu zakresie tematycznym.

Zarząd PISA postanawia skierować treść oświadczenia do Prezesa Polskiego Komitetu Normalizacyjnego, Przewodniczącego Komitetu Technicznego 52 PKN, Prezesa Krajowej Izby Gospodarczej, Prezesa Zarządu Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm", Prezesa Zarządu Polskiej Izby Ochrony Osób i Mienia, Prezesa Zarządu Polskiego Związku Pracodawców „Ochrona", Członków Polskiej Izby Systemów Alarmowych oraz branżowych czasopism i portali internetowych.

Bezpośr. inf.
Zarząd PISA

Inteligentny system zarządzania ruchem drogowym **Reg-Odyssey**

Bosch Security Systems przedstawia zaprojektowany na potrzeby branży transportowej system **Reg-Odyssey** – w pełni zintegrowane rozwiązanie z zakresu inteligentnego monitorowania ruchu pojazdów.

Reg-Odyssey to system służący do przechwytywania obrazów tablic rejestracyjnych REG. Posiada wbudowany moduł przetwarzania i ma możliwość transmisji obrazów i danych. Wszystko to dzięki jednemu wytrzymałemu i odpornemu na warunki pogodowe urządzeniu. Znajduje ono zastosowanie w szeregu rozwiązań w branży transportowej, w tym w monitorowaniu czasu podróży oraz nadzorowaniu ruchu drogowego i parkingów.

Dzięki swemu zasięgowi (8–25 m) system Reg-Odyssey umożliwia całodobowe przechwytywanie obrazów tablic rejestracyjnych pojazdów poruszających się z prędkością do 160 km/h. Wbudowany moduł przetwarzania stale monitoruje docelowy obszar pod kątem rozpoznawania przedniej i tylnej tablicy rejestracyjnej oraz przechwytywania obrazu pojazdów poruszających się w przeciwnych kierunkach.

System Reg-Odyssey nie wymaga niezależnego wyzwalania, dlatego pętle indukcyjne czy radary do obserwowania pojazdów stojących lub znajdujących się w ruchu nie są konieczne.

Wbudowany moduł przetwarzania umożliwia przechwytywanie danych z prędkością do 3600 tablic rejestracyjnych na godzinę. Przesyłane w formacie XML dane są przekazywane do centrów kontroli ruchu za pośrednictwem sieci WLAN, GPRS lub TCP/IP (10/100 Mb/s).

Bezpośr. inf. Emilia Dobies
Bosch Security Systems

Nowy rejestrator sieciowy Sony

Firma **Sony**, wychodząc naprzeciw wymaganiom rynku, wprowadziła następcę sieciowego rejestratora NSR (*Network Surveillance Recorder*) – serię urządzeń **NSR-1000**, które pozwolą na integrację istniejącego systemu analogowego z systemem IP. Są to urządzenia proste w implementacji i obsłudze. Wystarczy podłączyć kamery, a NSR sam wyszukuje adresy IP. Cały system bazuje na oprogramowaniu Real Shot Manager, które ma prosty i intuicyjny w obsłudze interfejs. Jest to hardware, software i wideoserwer w jednym. NSR jest urządzeniem pozwalającym korzystać z wielu funkcji, między innymi z zaawansowanej inteligencji, podglądu i zapisu obrazu z kamer. Urządzenie ma wejścia analogowe (BNC), wejścia sieciowe oraz możliwość konwertowania sygnału z analogowego na IP. Dzięki temu do jednego urządzenia można podłączyć oba rodzaje kamer: analogowe oraz sieciowe. Model NSR-1200 ma pojemność dysku 2 TB, do urządzenia można podłączyć 64 kamery IP, 16 kamer analogowych, a rejestrator zapewnia kompresję JPEG/MPEG-4. Dodatkowo Sony wprowadziło do oferty zewnętrzne macierze dyskowe SAS o symbolu NSRE -S200. Do jednego serwera można podłączyć siedem macierzy, każdą o pojemności 2 TB.

Bezpośr. inf. Marta Małecka
Sony Poland

Kompleksowa instalacja systemów bezpieczeństwa

Nowy europejski węzeł komunikacyjny frachtu lotniczego międzynarodowej firmy kurierskiej DHL International zlokalizowany na lotnisku Lipsk/Halle w Niemczech zaufał rozwiązaniom **Bosch Security Systems**. Umowa obejmuje całościową instalację niskoprądową systemu sygnalizacji pożarowej i dźwiękowego systemu ostrzegawczego.

Największym wyzwaniem w realizacji projektu była duża kubatura budynku. Z powodu określonych z góry warunków cyrkulacji powietrza w hangarze o wysokości 30 m zainstalowano specjalne czujki płomieni. Bosch wyposażył również stację paliw należącą do firmy DHL w system sygnalizacji pożarowej. Obszar węzła komunikacyjnego frachtu lotniczego jest monitorowany przez ponad 3000 czujek pożarowych łącznie. Dołączone są one do dwóch głównych central UGM 2020 i pięciu central sygnalizacji pożarowej serii BZ 500 LSN.

Cały system alarmowy monitorowany jest przez system zarządzania w pomieszczeniu sterującym firmy DHL. Do informacji podawanych przez system ma dostęp również lotniskowa straż pożarna. Aby zapewnić efektywne przekazywanie komunikatów głosowych we wszystkich budynkach, zainstalowano cyfrowy dźwiękowy system ostrzegawczy Praesideo. System złożony jest z kilku połączonych siecią paneli sterujących i dysponuje całkowitą mocą wyjściową powyżej 30000 W.

Węzeł komunikacyjny frachtu lotniczego w Lipsku jest jednym z trzech centralnych punktów przeładunkowych firmy DHL International obsługujących frachty lotnicze na całym świecie. Każdej nocy przesyłki ekspresowe w Lipsku obsługuje nawet 60 ekspresowych samolotów transportowych.

Bezpośr. inf. Emilia Dobies
Bosch Security Systems

Odpady z gospodarstw domowych zamieniane w energię elektryczną i cieplną w zabezpieczonym środowisku

Firma **Bosch** dostarczyła i zainstalowała systemy bezpieczeństwa w elektrowni zasilanej paliwem odnawialnym w parku przemysłowym Sonne/Großräschen w Lausitz (Niemcy), obsługiwanej przez przedsiębiorstwo E.ON Energy From Waste. Elektrownia produkująca energię elektryczną i cieplną z odpadów pochodzących z gospodarstw domowych została zaopatrzona w system dozorowy Bosch wyposażony w najnowszą technologię transmisji obrazu przez sieć IP i nowoczesny system sygnalizacji pożarowej.

Kamery Dinion (około 40) i kamery kopułkowe 360° przekazują obrazy ze wszystkich krytycznych obszarów w elektrowni. Nadmiarowe sieciowe rejestratory wizyjne zapewniają stały zapis obrazu. W przypadku niższych przepustowości sieci proces kompresji MPEG-4 gwarantuje uzyskanie obrazów bieżących o wyjątkowo wysokiej jakości. Dzięki systemowi zarządzania obrazem Bosch Video Management System personel ochrony ma zawsze pełny przegląd sytuacji na trzech stacjach roboczych, z których każda wyposażona jest w trzy monitory. Umożliwia to np. wyświetlanie na monitorach obrazów bieżących z procesu ważenia wszystkich wjeżdżających śmieciarek.

Technologia transmisji obrazu przez sieć IP firmy Bosch umożliwia podgląd procesów mających miejsce w elektrowni już kilka sekund po ich rzeczywistym wystąpieniu, zarówno lokalny, jak i zdalny. Już w początkowej fazie przetwarzania operator w elektrowni ma możliwość śledzenia na stronie sieciowej postępu interesujących go procesów przy użyciu jednej z kamer sieciowych.

Ochrona przeciwpożarowa również odgrywa kluczową rolę w koncepcji bezpieczeństwa elektrowni. Firma Bosch zainstalowała trzy uniwersalne centrale pożarowe UEZ 2000, które umożliwiają zapis ponad 300 komunikatów z czujek automatycznych i ręcznych ostrzegaczy pożarowych oraz przekazywanie kompleksowych komunikatów sterujących do systemów gaśniczych. Połączenie ze strażą pożarną zapewnia krótki czas reakcji w przypadku wystąpienia zdarzenia.

System zarządzania bezpieczeństwem firmy Bosch łączy system sygnalizacji pożarowej z wizyjnym systemem dozorowym, zapewniając zarządzanie obydwoma systemami przy pomocy standardowego, łatwego w obsłudze interfejsu. W przypadku pożaru zagrożone obszary są automatycznie wyświetlane na ekranach.

Energia elektryczna dla 38000 gospodarstw domowych

Centrum przemysłowo-komercyjne Sonne w Großräschen było wcześniej siedzibą fabryki cegieł i elektrowni Sonne. Elektrownia ta została zamknięta w roku 2004 z powodu wyczerpania złóż węgla w Meuro. W miejscu przestarzałej powstała nowoczesna elektrownia zasilana paliwem odnawialnym (śmieciami), produkująca obecnie 102 MW energii cieplnej i 24 MW energii elektrycznej na godzinę – wystarczająco dużo prądu, by zasilić 38000 gospodarstw domowych. Przed wybudowaniem tej elektrowni konieczne było wykonanie zakrojonych na szeroką skalę prac renowacyjnych i adaptacyjnych. W cały projekt zainwestowano ok. 90 milionów euro.

Bezpośr. inf. Emilia Dobies
Bosch Security Systems

FUSION – najnowsze niskonapięciowe oświetlacze firmy Raytec

LIGHT MATTERS raytec

Firma **Raytec** wprowadziła na rynek swoją ostatnią innowację w dziedzinie oświetlenia – **FUSION**.

FUSION, asortyment niskonapięciowych oświetlaczy zapewniających światło białe oraz podczerwień, zaprojektowano w celu uzyskania lepszego funkcjonowania dowolnych systemów kamerowych podczas pracy nocnej. Oświetlacze z tej serii są łatwe w instalacji, nie wymagają konserwacji i zapewniają wyjątkowo długą pracę.

W konstrukcji FUSION wykorzystano najnowsze rozwiązanie **PLATINUM LED** z miniaturowym układem optycznym, zastosowanym dla uzyskania mocy i parametrów na najwyższym światowym poziomie. Dzięki zastosowaniu w oświetlaczach technologii Command and Control użytkownik ma możliwość uzyskania najlepszego obrazu za każdym razem.

FUSION łączy w jednym urządzeniu, wymagającym jedynie zasilania stałego lub zmiennego o napięciu 12–24 V, technologię oświetlenia i sterowania zasilaniem firmy Raytec. Do zasilania oświetlaczy z tej serii nie jest wymagany oddzielny specjalizowany zasilacz. Każdy oświetlacz jest wyposażony w Active LED Life Control – układ do precyzyjnego sterowania sygnałem wyjściowym LED, zapewniający przewidywany czas działania urządzenia rzędu 10 lat.

FUSION jest **najważniejszym nowym opracowaniem firmy Raytec** od czasu wprowadzenia na rynek telewizji dozorowej produktów RAYMAX i RAYLUX. Oświetlacze FUSION zapewniają obrazy nocne najwyższej światowej klasy, umożliwiając jednocześnie łatwą, bezpieczną i szybką instalację.

– Opracowanie FUSION to wynik bezpośredniego sprzężenia zwrotnego ze strony profesjonalistów branży zabezpieczeń, którzy potrzebowali niskonapięciowych oświetlaczy o najlepszych parametrach. Nazwa FUSION oznacza, że technologie zasilania i oświetlenia firmy Raytec zostały połączone w jednym elastycznym i niezawodnym urządzeniu o dużych możliwościach – powiedział **David Lambert**, dyrektor ds. sprzedaży i marketingu w firmie Raytec.

Źródło: Bezpośr. inf. Raytec
Tłumaczenie: Adam Bułaciński, Redakcja

ULISSE IR360 – monitoring nocny w nowej wersji

Na ostatnich targach SICUREZZA w Mediolanie firma **VIDEOTEC** pokazała przykłady licznych innowacji dotyczących m.in. monitoringu nocnego i produktu o nazwie **ULISSE IR360**. Od teraz system ULISSE wraz z oświetlaczami podczerwieni zapewnia ciągły obrót, a więc połączenie nocnego monitoringu w zakresie 360° z cieszącą się uznaniem precyzją i niezawodnością całej rodziny ULISSE.

Te zewnętrzne systemy pozycjonujące są używane i doceniane w tysiącach instalacji na całym świecie, gdyż łączą zalety tradycyjnych głowic PTZ, takie jak wytrzymałość, sztywność, wysokiej jakości napędy itp., z szybkością i elastycznością, które są charakterystyczne dla kamer obrotowych. Pracowitość i staranność ekspertów-inżynierów, którzy dokładają starań, aby ulepszyć i rozszerzyć asortyment produktów firmy VIDEOTEC, jest gwarancją sukcesu tego produktu.

Bezpośr. inf. VIDEOTEC

Tłumaczenie: Adam Bułaciński, Redakcja

ULISSE w wersji MAXI

ULISSE MAXI to najnowszy członek rodziny ULISSE przeznaczony zwłaszcza do współpracy z dużymi kamerami i największymi obiektywami typu zoom, takimi jak: BOSCH 18x, FUJINON 22x, COMPUTAR 30x, PENTAX 20x.

System pozycjonowania integruje wyjątkowo dużą obudowę, głowicę do sterowania obrotu i uchyłu (P&T) oraz odbiornik telemetrii. Dzięki swojemu unikatowemu i regulowanemu systemowi przeciwwagi gwarantuje on optymalną pozycję kamery w zastosowaniach zewnętrznych.

Obrót w poziomie następuje w sposób ciągły ze zmienną szybkością do 20°/s, podczas gdy amplituda w osi pionowej zmienia się od –45° do +20° z maksymalną szybkością 20°/s. Wbudowana wycieraczka nie ogranicza pola widzenia kamery. ULISSE MAXI steruje funkcjami automatycznego obrotu w poziomie i patrolu z dokładnością przywołanej pozycji równą 0,02°. W celu uzyskania dokładnego pozycjonowania w każdych warunkach ULISSE MAXI wykorzystuje kodery optyczne zarówno do funkcji obrotu, jak i uchyłu. W wersji ULISSE MAXI oprócz tradycyjnego sterowania przez interfejs RS485 możliwe jest sterowanie obrotu, uchyłu i zbliżenia za pomocą IP oraz pełna integracja w systemie sieciowym.

Typowe instalacje obejmują kontrolę wizyjną w portach, zastosowania miejskie, przemysłowe, sportowe (na stadionach), w obiektach wojskowych i zakładach karnych. Dodatkowe informacje są dostępne na stronie www.videotec.com.

Bezpośr. inf. VIDEOTEC

Tłumaczenie: Adam Bułaciński, Redakcja

Szeroka oferta akcesoriów firmy Sony

By wyjść naprzeciw oczekiwaniom rynku, firma **Sony** dynamicznie wprowadza do swojej oferty coraz to nowsze produkty: kamery IP (tylko w roku 2008 zostały wprowadzone trzy kamery megapikselowe, jak również kamery obrotowe, w tym jedna z zoomem optycznym 36x) oraz oprogramowanie Real Shot Manager, które jest cały czas udoskonalane, o czym świadczy popularność kolejnych wersji. Niemniej jednak nie zapomina o istniejących systemach i wprowadza na rynek produkty, które umożliwią łatwą integrację istniejących systemów z najnowocześniejszymi technologiami. Takim produktem, ostatnio wprowadzonym na rynek, jest SNCA-COAX/DC/RV – inteligentny adapter ethernetowy. Urządzenie to zostało stworzone dla klientów, którzy chcieliby przenieść istniejący system analogowy do świata IP. Umożliwia podłączenie i zasilanie kamery IP poprzez istniejący kabel koncentryczny. Urządzenie podłączone do kabla koncentrycznego pozwala na korzystanie z pełnej prędkości przesyłania danych w sieci Ethernet, jak również daje możliwość zasilania kamer metodą Power over Ethernet (PoE). Technologia ta polega na konwertowaniu wychodzącego i wchodzącego sygnału symetrycznego na sygnał niesymetryczny, który następnie jest łączony i przesyłany poprzez pojedynczą wiązkę miedzianą. Kompensacja strat, jakie mają miejsce podczas konwertowania i łączenia, eliminowana jest poprzez proces powtórnego wzmocnienia. Instalacja SNCA-COAX/DC/RV zajmuje około pięciu minut, a pozwala przesyłać obraz z nawet czterech kamer! Odległość zależy od rodzaju kabla koncentrycznego, maksymalnie może wynosić 350 metrów. Urządzenie może być jedno- lub czteroportowe.

Oferta firmy Sony powiększyła się też o kolejne obudowy: SNCA-HFIXSML/24 oraz SNCA-HFIXSML/230 – małe obudowy do kamer stałopozycyjnych. Oprócz tego oferowane są również standardowe obudowy SNCA-HFIXSTD/24 i HFIXSTD/230. Wszystkie wymienione obudowy mają grzałkę, przyciemnianą szybkę, wieszak do ściany oraz klasę szczelności IP66.

Firma Sony wprowadziła na rynek również urządzenia emitujące światło podczerwone i białe. Urządzenie emitujące światło podczerwone o fali 700 nm lub dłuższej sprawia, że kamera chwyta światło niewidzialne dla ludzkiego oka. Pozwala to na pracę kamery w warunkach słabego oświetlenia. Wybór urządzenia emitującego (światło podczerwone lub białe) zależy od rodzaju kamery. Dostępne produkty mają następujące oznaczenia: SNCA-IR20, SNCA-IR20/OUTDR, SNCA-IR40/OUTDR, SNCA-IR80/OUTDR, SNCA-WL15/OUTDR.

Bezpośr. inf. Marta Małecka
Sony Poland

Siemens zapewnia bezpieczeństwo producentowi turbin wiatrowych

Siemens ukończył ostatnio kompleksowy i w pełni interoperacyjny **system bezpieczeństwa dla producenta turbin wiatrowych** w południowej Hiszpanii. Firma opracowująca i produkująca w jednym z najmniej uprzemysłowionych regionów Hiszpanii turbiny wiatrowe oraz łopaty śmigieł stanowi, z ponad 20000 metrami kwadratowymi swoich instalacji, jedno z najbardziej prestiżowych miejsc wdrażania innowacji w sektorze energii wiatrowej.

Dostarczony przez Siemensa system bezpieczeństwa stanowi rozwiązanie „pod klucz", zapewniające zarządzanie bezpieczeństwem całej fabryki z jednego centrum nadzoru (z dodatkowym centrum zapasowym). W związku z planami rozwoju fabryki istotne jest, aby system mógł być w przyszłości rozszerzony i aby obejmował także nowe obszary przy zachowaniu tych samych kryteriów bezpieczeństwa. Kompleksowy projekt obejmuje system dozoru wizyjnego SISTORE CX, kontrolę dostępu SiPass oraz systemy detekcji serii Sintony 400, przy czym wszystkie te systemy są zintegrowane przez unikatowy system MM8000 służący do zarządzania zagrożeniami (DMS – *Danger Management System*).

Firma Siemens zaangażowała się w inżynierię, zaprojektowanie, instalację i sprawdzanie działania systemu i, zgodnie z warunkami kontraktu, zapewnia prewencyjną konserwację oraz naprawy systemu w zakresie:

– systemu dozoru wizyjnego, obejmującego 24 stałe kamery w obudowach kopułkowych (standardowych i miniaturowych), podłączone do inteligentnego kodera SISTORE CX8 firmy Siemens w celu uzyskania transmisji pełnego strumienia wideo wysokiej jakości i zapisu obrazu z wykorzystaniem technologii MPEG4;

– wyjątkowo elastycznego i przyjaznego w obsłudze systemu kontroli dostępu SiPass firmy Siemens, monitorującego 16 przejść i umożliwiającego nadawanie praw dostępu według określonych kategorii oraz pełny wybór raportów;

– systemu detekcji Sintony 411ES, obejmującego 38 dualnych czujek ruchu chroniących biura, wyjścia awaryjne i otoczenie budynku, jeden detektor sejsmiczny do ochrony sejfu, trzy przyciski antynapadowe, umożliwiające natychmiastowe powiadomienie centrum nadzoru w przypadku problemów w recepcjach budynków, oraz dwie klawiatury do zapewnienia elastycznej obsługi.

Producent turbin ma na miejscu swoje własne centrum nadzoru, z którego monitoruje wszystkie budynki z wykorzystaniem systemu MM8000 firmy Siemens. W przypadku wystąpienia zdarzenia związanego z bezpieczeństwem obiektu system ten prowadzi obsługę przez zdefiniowane wcześniej kroki procedury obsługi zdarzeń.

Więcej informacji na temat rozwiązań oferowanych przez firmę Siemens można znaleźć na *www.siemens.com/securityandsafety*.

Źródło: www.securityworldhotel.com
Opracowanie: Adam Bułaciński, Redakcja

Nowa wyjątkowo duża obudowa do kamer – model HGV firmy VIDEOTEC

VIDEOTEC ma przyjemność zapowiedzieć **największą swoją obudowę do kamer – model HGV**. Dzięki jej dużym wymiarom mieszczą się w niej największe dostępne obecnie na rynku telewizji dozorowej obiektywy typu zoom.

Mocna konstrukcja obejmuje podstawę wykonaną z odlewu aluminiowego oraz górną część zawierającą osłonę przeciwsłoneczną wykonaną z wytrzymałego tworzywa ABS. Wycieraczki stanowią integralną część obudowy i nie ograniczają pola widzenia kamery.

Właściwa temperatura wewnątrz obudowy jest utrzymywana za pomocą wzmocnionego potrójnego grzejnika i dwóch dmuchaw pracujących w sposób ciągły dla zapewnienia obiegu powietrza wewnątrz obudowy.

Dzięki zastosowaniu, w celu zapewnienia mocnego zamykania obudowy, uszczelki neoprenowo-gumowej oraz śrub wykonanych ze stali nierdzewnej gwarantowana jest klasa odporności IP66.

Możliwe jest usunięcie utrzymywanej przez mocną linę bezpieczeństwa górnej części obudowy w celu uzyskania łatwego dostępu do wnętrza obudowy podczas jej instalacji oraz umożliwienia regulacji kamery.

Obudowa HGV jest idealnym rozwiązaniem do zastosowań zewnętrznych, takich jak monitoring pożarowy, bezpieczeństwo publiczne, systemy dozoru wizyjnego portów, wybrzeży, lotnisk i granic.

Bezpośr. inf. VIDEOTEC
Tłumaczenie: Adam Bułaciński, Redakcja

Finał VII i start VIII edycji studiów podyplomowych na **Wydziale Mechatroniki WAT**

W dniu 22 listopada 2008 r. **na Wydziale Mechatroniki** (WMT) **Wojskowej Akademii Technicznej** (WAT) w Warszawie miało miejsce **uroczyste zakończenie VII edycji niestacjonarnych studiów podyplomowych** pn. „Ochrona osób i mienia" oraz „Bezpieczeństwo lokalne i zarządzanie kryzysowe", połączone z **inauguracją ich VIII edycji**. Studia te, organizowane od 2001 r. przez Instytut Techniki Uzbrojenia WMT WAT we współpracy ze Studium Ochrony Osób, Mienia i Usług Detektywistycznych „CRIMEN II", są przeznaczone dla osób pracujących na stanowiskach związanych m.in. z: ochroną osób, mienia i informacji niejawnych oraz administrowaniem systemami bezpieczeństwa na poziomie lokalnym (przedsiębiorstwa, jednostki ratownictwa, straż miejska, administracja terenowa itp.).

Podczas uroczystości dziekan WMT WAT prof. dr hab. inż. Radosław Trębiński i dyrektor ITU WMT WAT prof. dr hab. inż. Józef Gacek, w obecności zaproszonych gości: prezesa CRIMEN II mgr. inż. pilota Eugeniusza Zduńskiego, redaktora naczelnego dwumiesięcznika *Zabezpieczenia* Teresy Karczmarzyk oraz wykładowców, wręczyli nowym studentom symboliczne indeksy, a absolwentom – świadectwa ukończenia studiów, a także uhonorowali nagrodami najlepszych. Studia z pierwszą lokatą ukończyła lic. Anna Tkaczyk, z drugą lokatą – mgr inż. Jerzy Tomaszewicz, natomiast z trzecią lokatą – ppłk mgr inż. Adam Marciniak. Gratulujemy!

VII edycję studiów ukończyło 30 absolwentów, a VIII edycję rozpoczęło 32 studentów.

Ryszard Woźniak

VII Zjazd Sprawozdawczo-Wyborczy Polalarm – relacja

W dniu 21 listopada 2008 roku w Warszawskim Domu Technika NOT odbył się **VII Zjazd Sprawozdawczo-Wyborczy OSIiTZTiZB „Polalarm”**.

Zjazd przyjął sprawozdania organów statutowych, określił kierunki działania na następne lata oraz wybrał nowe władze Stowarzyszenia.

W skład zarządu weszli:

- Bogdan Tatarowski – prezes,
- Krzysztof Ciesielski – wiceprezes,
- Andrzej Ryczer – wiceprezes,
- Andrzej Starnawski – wiceprezes,
- Jarosław Siemiątkowski – wiceprezes,
- Stefan Zaremba – sekretarz generalny,
- Krzysztof Borowy – członek,
- Marian Hady – członek,
- Mirosław Prokocki – członek,
- Jacek Szewczyk – członek,
- Andrzej Wójcik – członek.

Na wniosek zarządu Federacja Stowarzyszeń Naukowo-Technicznych NOT przyznała Srebrne Honorowe Odznaki NOT Andrzejowi Barcikowskiemu, Markowi Blimowi, Krzysztofowi Ciesielskiemu oraz Piotrowi Makowskiemu. Odznaki zostały wręczone przez prezesa Wojciecha Ratyńskiego oraz zastępcę sekretarza generalnego Włodzimierza Hausnera.

Z okazji Zjazdu zarząd Stowarzyszenia wyróżnił Dyplomami Uznania 39 działaczy Stowarzyszenia oraz 15 firm za ich osiągnięcia techniczne.

W czasie Zjazdu odbyła się uroczystość wręczenia szabli oficerskiej – przyznanej przez Krajowe Stowarzyszenie Ochrony Informacji Niejawnych – prezesowi zarządu Polalarm Bogdanowi Tatarowskiemu za wkład pracy w rozwój technicznej ochrony osób i mienia. Aktu wręczenia szabli dokonał gen. dyw. Zbigniew Bielewicz, akt nadania odczytał i wręczył prezes zarządu Tadeusz Koczkowski.

Bezpośr. inf. OSIiTZTiZB „Polalarm”

Więcej informacji ze Zjazdu, referat programowy zarządu, a także fotogalerię można znaleźć na naszej stronie *www.zabezpieczenia.com.pl* – zapraszamy.


SPRAWOZDAWCZO
-WYBORCZY
Ogólnopolskiego Stowarzyszeni
Inżynierów i Techników
Zabezpieczeń Technicznych
i Zarządzania Bezpieczeństwem
"POLALARM"


GRATULACJE
I NAJLEPSZE ŻYCZENIA
inż. Bogdana TATAROWSKIEGO


"POLALARM"

To już 20 lat firmy GUSTAW SECURITAS

No i mamy okrągłą rocznicę. Firma **Gustaw Securitas** obchodzi swoje **dwudziestolecie**. Ze względu na to, że w naszej obecnej rzeczywistości gospodarczej nie ma zbyt wiele firm z takim stażem, warto pokusić się o kilka refleksji i wspomnień. Pomysł zajęcia się ochroną osób i mienia zrodził się w głowie Gustawa Wilińskiego, który przekonał do niego Krystiana Soszkę. Przez kilka miesięcy odwiedzali różne instytucje, spełniali różne urzędnicze wymagania, co zaowocowało w końcu rejestracją spółki w sądzie. Ponieważ w 1988 r. trzeba było zostać rzemieślnikiem, żeby założyć firmę, założyciel spółki zapisał się do Cechu Rzemiosł Różnych w zawodzie kominiarz, ponieważ w tej profesji było wolne miejsce w cechu.

Pierwsze biuro mieściło się w wynajętym małym pokoju na peryferiach Szczecina. Założyciele pozyskali pierwszych klientów, zatrudnili pierwszych pracowników. Oferowali ochronę fizyczną, konwojowanie wartości pieniężnych. Im więcej potencjalnych klientów dowiadywało się o istnieniu firmy, tym szybciej rosło zainteresowanie samą firmą i świadczonymi przez nią usługami. Właściciele szybko zdali sobie sprawę, że ich przyszłość tkwi w nowoczesności, w oferowaniu klientom usług opartych na najnowszej technice elektronicznej. Jednak w Polsce takie rozwiązania nie były ani dostępne, ani szerzej znane. Trzeba było sięgnąć po doświadczenia zagraniczne.

Gustaw Securitas była pierwszą firmą, która zwróciła się do Amerykańskiego Funduszu Rozwoju Przedsiębiorczości o pomoc w zakupie stacji monitorowania systemów alarmowych. Otrzymała pożyczkę. Był to przełomowy moment w jej rozwoju, choć droga do sukcesu była jeszcze daleka. Wiązało się to nie tylko z rozwojem infrastruktury i zaplecza logistycznego, pozyskiwaniem wykwalifikowanych kadr, wdrażaniem skutecznych procedur działania. Szybko okazało się, że dużo wysiłku wymaga przekonywanie klientów, że monitorowany system alarmowy jest skuteczniejszy od tradycyjnych sposobów ochrony. Dzisiaj trudno w to uwierzyć, gdyż wiedza o możliwościach elektronicznej ochrony jest już powszechna.

Stawianie na nowoczesność i stałe doskonalenie procedur działania zawsze było i jest priorytetem firmy. To jedyny sposób na to, by nie pozostać w tyle i sprostać rosnącym oczekiwaniom klientów. A tych firma liczy już w tysiącach. Swym zasięgiem obejmuje bez mała całe dawne województwo szczecińskie.

Jak dziś wygląda firma, która dwadzieścia lat temu zaczynała od małego biura w wynajętym pokoju? Pracuje w niej około 400 osób. Kilkadziesiąt zmotoryzowanych patroli interwencyjnych przez okrągłą dobę jest gotowych do natychmiastowej reakcji na sygnał z alarmowego centrum odbiorczego o włamaniu czy jego próbie. Mobilność patroli interwencyjnych zapewnia klientom firmy **Gustaw Securitas System** najskuteczniejszą z możliwych ochronę ich firm, domów, biur, sklepów, a nawet terenów wokół różnych obiektów. Wielu włamywaczy trafiało i nadal trafia w ręce policji dzięki pracownikom Gustaw Securitas System. I nic w tym dziwnego. Oni są na ogół pierwsi na miejscu przestępstwa. Zjawiają się dyskretnie, bo takie możliwości daje system alarmowy i jego całodobowe monitorowanie. Pracownicy zatrudnieni bezpośrednio w ochronie fizycznej i elektronicznej mają kwalifikacje potwierdzone państwowymi licencjami, a cała firma posiada certyfikat ISO, otrzymany za jakość świadczonych usług. Dziś średnia wieku pracowników Gustaw Securitas System nie przekracza trzydziestu lat, a dziewięćdziesiąt procent kadry technicznej stanowią ludzie z wyższym

wykształceniem. Można więc rzec, że już drugie pokolenie ma swój udział w rozwoju firmy, jej otwarciu na nowoczesność, codzienne doskonalenie pracy. Spora grupa klientów jest wierna firmie od samego początku. Dają oni najlepsze świadectwo jej dbałości o ich mienie i poczucie bezpieczeństwa. Przyszłość firmy związana jest z nieustannym postępem, wdrażaniem najnowocześniejszych rozwiązań technicznych. Ochrona osób i mienia, w której najważniejszą rolę odgrywa elektronika, wymaga ludzi potrafiących się nią posługiwać. Ale takie uwarunkowania zawsze obowiązywały i obowiązują. Dlatego też Gustaw Securitas System z optymizmem patrzy w przyszłość.

I ma ku temu bardzo solidne podstawy. Dyrektor ds. technicznych w Gustaw Securitas System – Krzysztof Borowy

– nieustannie śledzi, co dzieje się w rozwoju światowej techniki dotyczącej szeroko pojętej ochrony osób i mienia. W firmie na bieżąco wdrażane są nowoczesne systemy, m.in. takie, które umożliwią nie tylko, jak dotąd, odbieranie sygnałów alarmowych z chronionych obiektów, ale też podgląd na ekranie monitora, który pozwala na obejrzenie, co było rzeczywistą przyczyną alarmu, dając jednocześnie możliwość utrwalania wizerunku sprawcy.

W firmie wdrożono i rozwijany jest system elektronicznej lokalizacji osób i pojazdów. Daje to szansę zwiększenia bezpieczeństwa. Na przykład zagubione dziecko wyposażone w maleńkie urządzenie zostanie zlokalizowane w kilka sekund. Dla osób starszych i niepełnosprawnych jest to również, w razie potrzeby, szansa na szybką pomoc. Możliwości wykorzystania takiego systemu monitorowania są praktycznie nieograniczone. Również dla firmy Gustaw Securitas System, której nowe technologie dają możliwość ciągłego rozwoju.

W celu uświetnienia okrągłej rocznicy współudziałowcy oraz zarząd zorganizowali spotkanie z pracownikami oraz zaproszonymi gośćmi, w tym także z klientami firmy. Podczas tego uroczystego spotkania, które urozmaiciły występy piosenkarki Ewy Kabzy oraz dzieci ze Szkoły Tańca „Astra", dzielono się wspomnieniami i rozmawiano o przyszłości firmy. Biorący udział w imprezie goście złożyli życzenia dalszych sukcesów i następnego takiego spotkania za kolejne 20 lat.

Do życzeń dołącza się cały zespół redakcji *Zabezpieczeń*.

Teresa Karczmarzyk

Jubileusz 10-lecia Schrack Seconet Polska

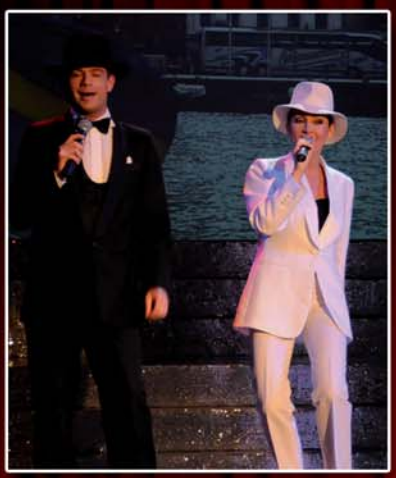
Z historii firmy

Schrack Seconet jest jednym z największych i najbardziej znanych producentów systemów ochrony przeciwpożarowej na świecie. Początki przedsiębiorstwa datuje się na okres wielkiej rewolucji przemysłowej XIX wieku, kiedy to na terenie dzisiejszej Austrii i Niemiec powstawały pierwsze zakłady produkujące urządzenia elektrotechniczne, które stanowiły podwaliny dzisiejszych koncernów nie tylko w Europie, ale również w Stanach Zjednoczonych czy Japonii. Nazwa firmy wywodzi się od nazwiska pomysłodawcy, przedsiębiorcy i naukowca, który zapoczątkował badania i konstruował pierwsze urządzenia radiotechniczne, stanowiące pierwowzory naszych dzisiejszych systemów sygnalizacji pożarowej. Już pierwsze lata XX wieku to rozwój zakrojonej na szeroką skalę produkcji prowadzonej przez Radiolaboratorium doktora Eduarda Schracka, która po przerwie wywołanej zniszczeniami II Wojny Światowej kontynuowana jest aż do dnia dzisiejszego. Sięgając do najważniejszych dat w rozwoju firmy na przestrzeni dziejów, należy koniecznie wspomnieć:

- lata siedemdziesiąte, kiedy to stworzono jedną z pierwszych na świecie sterowanych mikroprocesorowo central sygnalizacji pożarowej;
- rok 1997, kiedy to Schrack Seconet przystąpił do jednego z największych koncernów z branży zabezpieczeń – Securitas AG, który stanowi dziś jedną z najważniejszych platform rozwoju branży bezpieczeństwa w ogóle;
- rok 1998, w którym powstał **Schrack Seconet Polska**, zastępując działające od połowy lat 80. na rynku polskim przedstawicielstwo firmy austriackiej i tym samym stając się od tej pory jedynym bezpośrednim reprezentantem producenta w naszym kraju.

W dniu 10 grudnia 2008 r. w Warszawie odbyła się uroczystość obchodów jubileuszu 10-lecia firmy Schrack Seconet

Spotkanie miało miejsce w Teatrze Sabat. Po oficjalnym powitaniu ponad 150 znakomitych gości, w tym m.in.: inwestorów, przedstawicieli firm partnerskich, instytucji, organizacji związanych z ochroną przeciwpożarową, specjalistów z branży zabezpieczeń oraz prasy, prezes zarządu **Grzegorz Ćwiek** zaprosił na scenę osoby, które wywarły ogromny wpływ na firmę od początku jej istnienia na rynku polskim. Oficjalna część spotkania, której firma nadała tytuł „Wspomnień czar…", miała charakter rozmowy – dyskusji wprowadzającej wszystkich gości w historię firmy i kolejne etapy jej rozwoju, a także przedstawiającej pozycję Schrack Seconet w chwili obecnej na rynku polskim i europejskim. O powodach zainteresowania rynkiem polskim na początku lat dziewięćdziesiątych i pierwszych kontaktach z przedstawicielami branży zabezpieczeń opowiedział ówczesny dyrektor generalny Schrack Seconet AG – Hans Zavesky. Przedstawiciele firmy austriackiej wiązali ogromne nadzieje z rozwojem swojego przedstawicielstwa w Polsce, a tym samym liczyli na zdobycie ogromnego rynku w tej części Europy. O pierwszym dużym obiekcie w Polsce, zabezpieczonym systemami Schrack Seconet hotelu Marriott w Warszawie, opowiedzieli panowie: Andrzej Jankowski, prezes firmy Fire-Max, oraz prezes firmy Futura – Zbigniew Nadecki. Obaj panowie byli pierwszymi osobami w Polsce, z którymi firma Schrack Seconet AG nawiązała bezpośrednią współpracę jeszcze w latach 80., i byli jej jedynymi przedstawicielami do połowy lat 90. Po utworzeniu oficjalnego przedstawicielstwa, Schrack Seconet Gmbh, firmy, które reprezentowali, stały się wiodącymi partnerami handlowymi producenta i do dziś pozostają w grupie



autoryzowanych partnerów Schrack Seconet Polska. O stanie wiedzy z zakresu zaawansowanych technologii przeciwpożarowych środowiska pożarniczego oraz uwarunkowaniach prawnych, decydujących o możliwościach wprowadzenia nowych systemów na rynek polski na początku lat dziewięćdziesiątych (w tym również o początkach tworzenia norm i obowiązujących do dziś aktów prawnych w dziedzinie zabezpieczeń przeciwpożarowych), opowiedział generał PSP (Państwowej Straży Pożarnej) w st. spoczynku, późniejszy Komendant Wojewódzki PSP, Roman Kaźmierczak. Do dyskusji dotyczącej początków certyfikacji urządzeń sygnalizacji w ogóle oraz produktów Schrack Seconet został zaproszony wieloletni pracownik Centrum Naukowo-Badawczego w Józefowie – Jerzy Ciszewski, obecnie pracownik Instytutu Techniki Budowlanej. W swojej wypowiedzi podkreślił on ogromny wkład firmy w rozwój laboratorium badawczego CNBOP w tamtych trudnych czasach dzięki wprowadzonemu przez firmę na rynek polski know-how i produktom – jak na owe czasy – bardzo zaawansowanym technologicznie. Rozmowę na temat rozwoju firmy w Polsce, jej ówczesnej i obecnej sytuacji na rynku polskim i europejskim, zakończyli panowie: Wolfgang Kern – obecny dyrektor generalny Schrack Seconet AG, Herbert Hübl – dyrektor ds. ksportu Schrack Seconet AG oraz Richard Pertschy – wieloletni opiekun m.in. rynku polskiego ze strony macierzystej firmy z Wiednia. Ich zdaniem firma Schrack Seconet Polska na przestrzeni ostatnich dziesięciu lat znacznie umocniła swoją pozycję dzięki szybkiemu, ale stabilnemu rozwojowi oraz ustanowieniu nowych standardów w dziedzinie zabezpieczeń.

Część oficjalną spotkania zakończyło wręczenie nagród i wyróżnień dla poszczególnych osób oraz firm najdłużej związanych z firmą Schrack Seconet Polska. Wyróżnienia-podziękowania „za niezwykle ważny wkład w budowę i rozwój firmy na przestrzeni 10 lat jej działalności w Polsce oraz wspólny udział w tworzeniu profesjonalnego rynku systemów bezpieczeństwa" otrzymały firmy: Fire-Max, Futura, G4S Security Systems (Polska) (dawniej: Falck Ochrona), Hoffman AD, Insap (dawniej: PUT Intel), PPHU Tel-Poż-System „ISKRA", NOMA 2, OBIS Cichocki Ślązak, Panorama-SAP, IPW Projex, Supo Cerber oraz Forestel.

Nagrody „za osiągnięcie najwyższych wyników sprzedaży systemów bezpieczeństwa Schrack Seconet w grupie Autoryzowanych Partnerów w latach 1998–2008 oraz wysoką jakość usług" otrzymały w kolejności firmy: Johnson Controls International, Qumak-Sekom, Futura. Specjalne wyróżnienie za wieloletnią owocną współpracę zostało przyznane Stowarzyszeniu Inżynierów i Techników Pożarnictwa.

Po części oficjalnej wszyscy goście zostali zaproszeni do obejrzenia specjalnie na tę okazję przygotowanego spektaklu w wykonaniu artystów Teatru Sabat pt. „Europa razem". W finale przedstawienia na scenę wjechał tort z racami, a wszyscy zebrani na sali goście złożyli wspólnie gratulacje firmie Schrack Seconet Polska, odśpiewując „Sto lat…". Wieczór zakończyły długie, miłe rozmowy i wspomnienia wszystkich zebranych gości.

Zespół Schrack Seconet Polska składa serdeczne podziękowania wszystkim, którzy przyczynili się do dynamicznego rozwoju firmy w Polsce. Dziękujemy szczególnie wszystkim gościom przybyłym na obchody jubileuszu 10-lecia, mając jednocześnie nadzieję na kolejne wspólne przedsięwzięcia i długoletnią współpracę.

Bezpośr. inf. Marta Nowak
Schrack Seconet Polska

IV Konferencja
Razem bezpieczniej

Tradycyjnie, jak co roku, w dniach 08–10.10.2008 r. odbyła się w województwie zachodniopomorskim czwarta już z kolei, organizowana wspólnie przez **Komendę Wojewódzką Policji w Szczecinie**, **Zarząd Wojewódzki Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych** i **Zarządzania Bezpieczeństwem „Polalarm”**, **Zarząd Wojewódzki Polskiej Izby Ochrony Osób i Mienia** oraz **Fundację „Razem bezpieczniej” IV Konferencja „Razem bezpieczniej”**.

W konferencji wzięło udział ponad dziewięćdziesięciu uczestników, w tym: przedstawiciele firm ochrony osób i mienia woj. zachodniopomorskiego, osoby funkcyjne odpowiedzialne za ochronę obiektów podlegających obowiązkowej ochronie, komendanci miejscy i powiatowi policji garnizonu zachodniopomorskiego.

Organizowana co roku konferencja cieszy się coraz większym uznaniem, o czym świadczy rosnąca liczba jej uczestników.

Po przywitaniu uczestników konferencji przez komendanta wojewódzkiego policji oraz prezesów zarządu wojewódzkiego „Polalarmu” i Fundacji „Razem bezpieczniej” przystąpiono do realizacji programu konferencji.

W ramach programu prowadzono ożywioną dyskusję wokół następujących problemów:

1. Uchybienia w działalności SUFO (Specjalistyczne Uzbrojone Formacje Ochronne – przyp. red.). Przedstawiciele Wydziału Postępowań Administracyjnych KWP w Szczecinie przedstawili sprawozdanie z kontroli działalności SUFO za rok 2007. Omówili tendencje w poszczególnych grupach zagadnień oraz najczęściej powtarzające się uchybienia. W ramach prowadzonej dyskusji wyjaśniono niektóre problemy związane z interpretacją przepisów.
2. Rola i miejsce rzeczoznawcy zabezpieczeń technicznych i zarządzania bezpieczeństwem w procesie opracowywania planów ochrony. Dyskutowano nad problemem przygotowania analizy zagrożeń oraz oceny stanu zabezpieczeń technicznych w ramach opracowywanych planów ochrony, a także o możliwościach współdziałania w tym zakresie z rzeczoznawcą lub wstępnego przygotowania tego typu analizy oraz oceny w osobnym dokumencie i wykorzystania wniosków z tejże analizy i oceny w planie ochrony obiektu.
3. Organizowanie się branży ochrony w Europie oraz usługi ochrony a regulacje europejskie. Przedstawiciele Polskiej Izby Ochrony Osób i Mienia przekazali informacje na ten temat, które mogą być pomocne dla firm ochrony oraz instytucji sprawujących nadzór nad funkcjonowaniem branży ochrony. Dyskutowano nad projektowaną przez Komisję Europejską dyrektywą mającą ułatwić świadczenie usług zarówno poprzez rozpoczęcie stałej działalności gospodarczej w innym państwie członkowskim, jak i świadczenie czasowe bez zmiany siedziby przedsiębiorstwa.
4. Zagrożenie bezpieczeństwa placówek bankowych i skuteczność stosowania środków zabezpieczających. Przedstawiciel Związku Banków Polskich omówił tendencje i nowe zagrożenia w działalności bankowej. Zaprezentował także statystykę tych zagrożeń. Przedstawił działania banków, które mają na celu zmniejszenie

zagrożeń oraz stosowanie coraz nowszych metod neutralizacji tychże zagrożeń.

5. Zagrożenie zamachami terrorystycznymi w placówkach bankowych. Specjalista do spraw terroryzmu omówił aspekty tego rodzaju działań, sposoby postępowania oraz kierunki działań prewencyjnych. Swoje wystąpienie urozmaicił filmem zrealizowanym podczas praktycznego szkolenia związanego z postępowaniem i zachowaniem się pracowników obiektu podczas zamachu terrorystycznego i wzięcia grupy zakładników.
6. Zagrożenia związane z informacjami o podłożeniu ładunku wybuchowego na terenie chronionego obiektu. Po omówieniu tych zagrożeń funkcjonariusze SPAP KWP w Szczecinie przedstawili algorytm postępowania. Omówili także znaczącą rolę pracowników ochrony w obiektach podlegających obowiązkowej ochronie, w obiektach użyteczności publicznej i obiektach handlowych wielkopowierzchniowych, w których obserwują oni niecodzienne zachowania i postępowanie klientów, które mogą świadczyć o istnieniu zagrożenia.
7. Działalność edukacyjna Fundacji „Razem bezpieczniej". Przedstawicielka fundacji omówiła problematykę szkoleniową z zakresu sytuacji kryzysowych w instytucjach, szkołach, obiektach handlowych, a także sposoby reagowania w tych sytuacjach. Posiłkując się prezentacją, omówiła realizowane cykle szkoleń.
8. Zasady transportowania wartości pieniężnych z zastosowaniem przepustki specjalnej „W". Naczelnik Wydziału Ruchu Drogowego KWP w Szczecinie omówił zasady wydawania przepustki „W" oraz korzystania z niej, mając na uwadze przepisy ustawy „Prawo o ruchu drogowym". W swojej prezentacji przedstawił wszystkie algorytmy postępowania w przypadku kontroli drogowej.
9. Zabezpieczenie imprez masowych w świetle obowiązujących przepisów. Posiłkując się posiadanymi materiałami filmowymi, przedstawiciel sztabu KWP w Szczecinie omówił wymogi dotyczące zabezpieczenia imprez masowych w świetle obowiązujących przepisów oraz ocenił stan spełnienia tychże wymogów w województwie zachodniopomorskim.
10. Współpraca pomiędzy kierownikami jednostek policji a firmami ochrony w zakresie wymiany informacji o zagrożeniach obiektów podlegających obowiązkowej ochronie. Temat ten, omówiony przez przedstawiciela WPA KWP, przedstawiciela Sztabu KWP w Szczecinie oraz przedstawiciela Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie, zajął najwięcej czasu i wywołał szeroką dyskusję. Omówiono go na przykładzie rzeczywistej sytuacji kryzysowej w województwie zachodniopomorskim – awarii sieci energetycznej. Poruszono problem ochrony obiektów w systemie dozoru sygnałów w przypadku braku łączności GSM w wyniku awarii zasilania. Jednym z wniosków końcowych tego panelu było stwierdzenie, że do zbierania informacji o sytuacji w terenie nie wykorzystano w pełni możliwości firm ochrony, które posiadają własną sieć powiadamiania i własne zasilanie awaryjne.

Program konferencji urozmaicono prezentacją urządzeń, systemów zabezpieczeń technicznych oraz oprogramowania. Prezentację zorganizowały firmy Netel oraz Progryf ze Szczecina.

Ponadto w godzinach popołudniowych zorganizowano dla uczestników konferencji występy aktorów Teatru Polskiego w Szczecinie.

W czasie dyskusji oraz podczas podsumowania konferencji zbierano wnioski i propozycje dotyczące organizacji V Konferencji „Razem bezpieczniej" w 2009 roku.

Obrady zakończono wręczeniem wszystkim uczestnikom wspólnej fotografii.

Bezpośr. inf. Krzysztof Borowy
Gustaw Securitas

Maxtel

– firma, która odniosła sukces

W bieżącym roku minęło dwadzieścia lat od powstania **kieleckiej spółki Maxtel**, znanej początkowo tylko w Kielcach i w regionie świętokrzyskim, później w całym kraju, a nawet poza jego granicami.

Jednym z pomysłodawców i twórców firmy był **Waldemar Kryś**, który dostrzegł potrzebę powołania jej w celu rozwoju usług telekomunikacyjnych w regionie. Firma stała się ewenementem na rynku, gdyż powstała w dobie najgłębszego kryzysu ekonomicznego w Polsce, która w 1988 roku stanęła na progu bankructwa gospodarczego.

Tym bardziej cieszy obchodzony w tym roku **jubileusz dwudziestolecia Maxtela**, który zgromadził w kieleckim Hotelu Kongresowym licznych kontrahentów firmy z całej Polski, przedstawicieli władz lokalnych oraz współpracowników i przyjaciół firmy. Ordynariusz kielecki ks. biskup Kazimierz Ryczan w swym wystąpieniu na uroczystej gali podkreślał moralne i humanistyczne oblicze firmy, która stawia zawsze najpierw na człowieka, a dopiero później na zysk i sukcesy ekonomiczne. Szef Staropolskiej Izby Przemysłowo-Handlowej Ryszard Zbróg z dumą podkreślał zasługi Maxtela związane z udziałem w dokonywaniu zmian technologicznych w regionie.

W podobnym duchu wypowiadał się dyrektor Wiesław Dzierżak z Centrum Usług Satelitarnych w Psarach: – *Pan dba o to, byśmy byli pełnoprawnymi obywatelami współczesnego świata* – powiedział, zwracając się do prezesa Waldemara Krysia.

Sukcesów gratulowali Maxtelowi szefowie największych firm z całej Polski, w tym prezes Kolportera Holding – Krzysztof Klicki.

Waldemar Kryś wspominał początki firmy – zakładanie Telewizji Kablowej Kielce i tworzenie jednego z pierwszych w Polsce studia telewizyjnego. Prezes podkreślił również, jak ogromne znaczenie w działalności biznesowej mają ludzie: – *Największą wartością naszej firmy są profesjonalnie przygotowani i emocjonalnie związani z firmą pracownicy.*

W XXI wieku Maxtel stawia przede wszystkim na rozwój systemów zabezpieczeń: automatycznych systemów sygnalizacji pożaru, dźwiękowych systemów ostrzegawczych, systemów sygnalizacji włamania i napadu, systemów monitoringu telewizyjnego, a także na integrację tych systemów w ramach jednolicie działającej struktury. Klientami firmy są dziś min. Volvo, Echo Investment, Mitex, Browar Belgia, Celsa Huta Ostrowiec, Tesco. O pozycji Maxtela na rynku gospodarczym świadczą liczne nagrody i wyróżnienia. Najważniejsze z nich to czterokrotny Medal Europejski i trzykrotna Gazela Biznesu.

Uroczystość dwudziestolecia firmy Maxtel uświetnił występ Kieleckiego Teatru Tańca ze spektaklem „Niemen". Po spektaklu zebranych gości zaproszono na bankiet do restauracji Patio w Hotelu Kongresowym.

Bezpośr. inf. Magdalena Kryś
Maxtel

NOWA SERIA REJESTRATORÓW
DOSTĘPNA W OFERCIE **CBC**

GANZ

produced by CBC

WORLD WIDE NETWORK

Nowa seria rejestratorów DRxxN2-DVD jest kontynuacją dobrze znanych rejestratorów DIGIMASTER.

Nowe modele charakteryzują się podwojoną szybkością rejestracji oraz obsługą dysków SATA.

- Nagrywanie z szybkością 200 klatek/sek.
- Obsługa DDNS oraz synchronizacja czasu NTP
- Indywidualna konfiguracja parametrów nagrywania
- Obsługa dysków wewnętrznych SATA

www.cbcpoland.pl

RACS ROGER ACCESS CONTROL SYSTEM

seria radius

CE

Seria Radius

Seria Radius to całkowicie nowa linia wzornicza czytników i kontrolerów dostępu zaprojektowana w oparciu o wieloletnie doświadczenie firmy Roger w tej dziedzinie.

W skład rodziny wchodzą czytniki i kontrolery różniące się konstrukcją mechaniczną oraz funkcjonalnością, w zależności od modelu obsługują one karty standardu EM 125 kHz lub 13,56MHz Mifare. Nową kategorię produktu stanowi wandalo-odporny czytnik (PRT64EM-VP) w którym przednia część obudowy i klawisze są wykonane w całości z metalu.
Na szczególną uwagę zasługuje kontroler PR602LCD specjalnie zaprojektowany dla systemów rejestracji czasu pracy RCP, do których oferowane jest nowoczesne oprogramowanie RCP Master.

RCP Master *PR602LCD*

RCP Master

Kompleksowe rozwiązanie RCP firmy ROGER ułatwia zarządzanie czasem pracy oraz wpływa na redukcję kosztów oraz precyzję rozliczania, przyczyniając się pośrednio do wzrostu produktywności w przedsiębiorstwie. RCP Master posiada łatwy w obsłudze, przyjazny interfejs. Program może być użytkowany bezpłatnie w celach ewaluacyjnych przez pierwsze 60 dni. RCP Master oferowany jest z licencją do obsługi 50, 250 lub powyżej 250 pracowników a także w wersji jedno lub wielostanowiskowej, co umożliwia dopasowanie rozwiązania do struktury i wielkości przedsiębiorstwa. Program RCP Master został opracowany w środowisku Microsoft .NET i jest przeznaczony dla systemów operacyjnych Windows XP i Vista.

profesjonalna kontrola dostępu

roger®

www.roger.pl

EASY RIDER

Bartłomiej Dryja

Z roku na rok, wraz z nastaniem wiosny, można zaobserwować na polskich drogach coraz więcej pojawiających się motocykli. Są to zarówno sportowe ścigacze, majestatyczne choppery, jak i zwinne skutery. Pęd do jednośladów nie przeszedł bez echa także wśród agencji ochrony. W niniejszym artykule postanowiłem przyjrzeć się z bliska temu zjawisku, przedstawiając zarówno wady, jak i zalety wyposażenia grup interwencyjnych w motocykle

ŹRÓDŁO ZAKUPU

Jeśli rozważa się zakup motocykli, dobrze jest skorzystać z doświadczeń instytucji posiadającej chyba największą praktykę w stosowaniu jednośladów w służbach patrolowych. Taką instytucją w naszym kraju jest z pewnością policja, która jeszcze przed II Wojną Światową używała motocykli. Była wśród nich między innymi kultowa polska konstrukcja, produkowany przez Centralne Zakłady Samochodowe ciężki motocykl marki Sokół. Dużo później, bo w 1961 roku, już za czasów milicji, trafił tam do użytku „polski Harley", czyli motocykl Junak. Ten ostatni został specjalnie zmodyfikowany, wyposażony dodatkowo w owiewki i zamontowaną z tyłu, zamiast siodełka pasażera, radiostację. Obecnie, przykładowo w Sekcji Ruchu Drogowego w Bielsku-Białej, są wykorzystywane cztery motocykle, jak podaje podoficer prasowy Komendy Miejskiej Policji w Bielsku-Białej podkomisarz Elwira Jurasz. W okolicznych komisariatach jest ich jednak znacznie więcej. W użyciu są zarówno lekkie motocykle Yamaha o pojemności 250 cm^3, jak i ciężkie Honda o pojemności 750 cm^3. Są to motocykle drogowe oraz enduro, wykorzystywane w trudnych warunkach górskich i leśnych. Wyboru dokonała Komenda Główna Policji, biorąc pod uwagę własności drogowe motocykli, warunki gwarancyjne oraz cenę. Patrole motocyklowe wyjeżdżają na drogi od wiosny do późnej jesieni, gdy temperatura wynosi ponad 5°C (co ciekawe – niezależnie od warunków atmosferycznych). Wcześniej wszyscy policjanci przechodzą jednomiesięczne szkolenie w Centrum Szkolenia Policji w Legionowie. Szkolenie to stanowi uzupełnienie dla posiadanego prawa jazdy kategorii A, upoważniającego do prowadzenia motocykla o pojemności silnika przekraczającej 50 cm^3. W ośrodku tym, na 56 hektarach, ćwicząc na specjalnie wybudowanym torze, policjanci zdobywają doświadczenie w kierowaniu pojazdem z uwzględnieniem niebezpiecznych manewrów oraz zdobywają podstawową wiedzę dotyczącą obsługi technicznej. Niestety, jak powiedziała Rzecznik Prasowa Policji, nie są tam przeprowadzane szkolenia dla osób z zewnątrz.

W jednym sezonie motocykle przejeżdżają około 4000 km i są użytkowane zarówno jako środek lokomocji patroli drogowych, jak i wsparcie organizowanych imprez masowych.

AGENCJE OCHRONY

Motocykle w agencjach ochrony nie są nowym zjawiskiem. Po raz pierwszy zetknąłem się z grupami interwencyjnymi na motocyklach jeszcze w trakcie swoich studiów w Krakowie w roku 2002. Były to patrole agencji ochrony Justus. Zgodnie z informacjami uzyskanymi od Pana Wojciecha Żurka, pierwsze motocykle w firmie Justus pojawiły się jeszcze w 2000 roku. Początkowo były to specjalnie sprowadzone z USA Kawasaki KZ 1000, teraz to Yamaha YZF, Suzuki V-Storm, Kawasaki ER 500 i nawet jeden egzemplarz Suzuki Hayabusa. Szczególnie ten ostatni motocykl jest interesujący, ponieważ jako pierwsza fabryczna konstrukcja na świecie jest zdolny przekroczyć 300 km/h, a 100 km/h osiąga w zaledwie 2,6 sekundy. Wracając jednak do agencji Justus, wykorzystywane są tam zawsze dwa motocykle równocześnie. Możemy je spotkać na drogach w okresie od marca do listopada, oczywiście w odpowiednich warunkach atmosferycznych. Jeśli chodzi o wymagania stawiane kierowcom, to są one zdecydowanie większe niż te w przypadku samochodów, bo wymagane jest zaliczenie specjalnego egzaminu, w którym bierze udział sam szef agencji ochrony Justus, który notabene sam jest miłośnikiem motocykli. Ze względu na ograniczoną pojemność bagażową motocykla ochroniarze są wyposażeni tylko w podstawowe środki przymusu bezpośredniego. W przyszłości planowane jest podłączenie modułów GPS, na razie jednak jedynym wyposażeniem dodatkowym są radiostacje z mikrofonogłośnikami wkładanymi bezpośrednio do ucha albo wbudowanymi w kask. Podobnie jest w przypadku motocykli używanych przez agencję ochrony Komes z Bielska-Białej. Od roku 2004 wykorzystywane są tam nieprzerwanie dwa motocykle Honda XL 600V Transalp. Jak zapewnia Kierownik Operacyjny Bronisław Obracaj, nie sprawiają one praktycznie żadnych problemów technicznych i jedynym mankamentem jest to, że nie można w nich zamontować instalacji gazowej w celu zmniejszenia kosztów eksploatacji.

ZALETY

Chyba największym i najistotniejszym plusem zastosowania motocykli w grupach interwencyjnych jest skrócenie czasu dojazdu. W większych aglomeracjach miejskich w godzinach szczytu praktycznie nie mamy szansy zapewnienia skutecznej, a więc szybkiej, interwencji. Rozważając wykorzystanie motocykli, powinniśmy więc kierować się przede wszystkim analizą czasów dojazdów. W mniejszych miejscowościach, w których samochodowe patrole zapewniają wymaganą mobilność, koszty poniesione z powodu wprowadzenia motocykli mogą okazać się nieuzasadnione. Tam zaś, gdzie korki zaczynają być codziennością, motocykle umożliwią skrócenie czasu dojazdu, a więc zdecydowanie podniesie się jakość usług świadczonych przez agencje ochrony. Jak podaje agencja ochrony Justus, czas interwencji na terenie Krakowa skrócił się dzięki motocyklom nawet o jedną trzecią w stosunku do czasu, którego potrzebowały patrole samochodowe.

Inną korzyścią jest stosunkowa łatwość poruszania się w trudnym terenie. Motocykle enduro docierają w miejsca absolutnie niedostępne dla pojazdów samochodowych. Jak już wspomniano wcześniej, walory te doceniła m.in. policja.

Nie należy też pomijać aspektu marketingowego całego przedsięwzięcia. Fiaty i skody, tak popularne w naszym kraju jako wozy grup interwencyjnych, nawet fantazyjnie opisane, nie zwracają już niczyjej uwagi. O ile więc nie planujemy zakupu pojazdów marki Ferrari dla załóg, aby stać się bardziej zauważalnymi, możemy zastosować motocykle, co zdecydowanie wyróżni agencję ochrony.

WADY

Oponenci idei zastosowania motocykli w grupach interwencyjnych zgłaszają wiele uwag. Podstawową i wymienianą często nawet przez zwolenników jest wrażliwość na warunki atmosferyczne. Dokładając do tego sezonowość zastosowania motocykli w naszym klimacie, uzyskujemy rozwiązanie, którego nie można traktować jako pełnego zamiennika patroli samochodowych. Patrolując w godzinach nocnych, lepiej korzystać z samochodów (ze względu na mniejszą wygodę, jaką zapewnia kierowcy motocykl, brak zabezpieczenia przed niższą temperaturą otoczenia i gorszą widoczność).

Dużym problemem jest też znalezienie odpowiednio przeszkolonych pracowników. Przy obecnych problemach kadrowych skompletowanie zespołu ludzi posiadających minimum prawo jazdy kategorii „A" stanowi nie lada problem.

Kolejną przeszkodą są koszty. W pierwszej chwili wydaje się, że rozwiązanie to jest bardziej ekonomiczne niż użycie samochodów. Zdecydowanie niższy niż w przypadku samochodu jest koszt przeciętnego motocykla, paliwa (przy spalaniu rzędu 4–5 litrów na 100 km) czy też roczny koszt ubezpieczenia. Niestety, koszty te należy liczyć podwójnie, jeżeli myślimy o wprowadzeniu dwuosobowych patroli. Każda z osób powinna posiadać swój własny motocykl, ponieważ podróż dwóch osób w pełnym rynsztunku na jednym motocyklu jest, delikatnie mówiąc, niewygodna.

W tym miejscu należy zwrócić uwagę na jeszcze jeden problem – kłopot z zabraniem dodatkowego wyposażenia oraz montażem coraz popularniejszych systemów nawigacji satelitarnej i palmtopów zapewniających cyfrową łączność z bazą. Owszem, można zamontować na motocyklu dodatkowe kufry i uchwyty, jednak korzystanie ze sprzętu tak przechowywanego jest niewygodne, zajmuje cenny czas, a sam sprzęt jest narażony na uszkodzenie.

Interesująco wygląda sprawa bezpieczeństwa. W powszechnym mniemaniu motocykle są pojazdami bardziej niebezpiecznymi i narażonymi na większą liczbę wypadków drogowych. Jednak, jak wynika z informacji uzyskanych w Komendzie Miejskiej Policji w Bielsku-Białej, statystycznie wypadki z udziałem służbowych motocykli, przy uwzględnieniu ich mniejszej liczby, zdarzają się rzadziej niż w przypadku samochodów. Potwierdzają to również pracownicy agencji ochrony Justus i Komes.

KOSZTY

Ze względu na liczbę oferowanych marek i modeli wybór motocykla jest nie lada problemem. Najrozsądniej jest wybrać motocykl uniwersalny – taki, który sprawdzi się zarówno na zatłoczonych ulicach miejskich, jak i w umiarkowanie trudnym terenie.

Taką konstrukcją jest z pewnością Honda XL700V Transalp. Historia tego motocykla sięga 1987 roku. Od tamtego czasu motocykl ten wielokrotnie się zmieniał, zwiększano pojemność silnika, moc, wzmacniano hamulce. Obecnie jest to motocykl z elastycznym silnikiem, dobrze zestrojonym zawieszeniem i w stosunkowo przystępnej cenie. Nowy egzemplarz kosztuje w salonie około 25900 zł, używany w dobrym stanie można nabyć już za 15000 zł. Mając wybrany motocykl, trzeba zastanowić się nad dodatkami.

Pierwszym elementem jest ubiór. Należy kupić kask oraz odpowiedni kombinezon składający się z kurtki, spodni, butów i rękawic. Rozbieżność cen w tym przypadku może być nawet kilkukrotna. Przykładem jest choćby kask. Może on kosztować 200 zł (Grex), 700 zł (Nolan) albo 1700 zł (Shoei). Dodatkowo należy pamiętać, że ubiory powinny być zakupione w liczbie odpowiadającej liczbie kierowców, a nie motocykli, chyba że pozwolimy na wykorzystywanie tego samego kombinezonu przez więcej niż jednego kierowcę.

Najtrudniejsze zadanie czeka nas jednak przy wyborze środków łączności radiowej. Stosowane są różnorakie rozwiązania. Najprostsze z nich to przenośny radiotelefon z mikrofonogłośnikiem, inne to specjalny zestaw nagłowny zintegrowany z kaskiem. Jedno i drugie rozwiązanie ma swoje wady. Pierwsze nie umożliwia łączności w trakcie jazdy, drugie jest kłopotliwe w trakcie interwencji, kiedy trzeba szybko zdjąć kask. Jak mówi Marek Friedrich z agencji ochrony Komes, problematyczne jest także automatyczne przechodzenie w tryb nadawania w przypadku zastosowania mechanizmu VOX. Często sam odgłos silnika potrafi uruchomić nadawanie. Ciekawym rozwiązaniem wydaje się zestaw nagłowny firmy SetCom, przystosowany specjalnie do motocykli i współpracujący z radiotelefonami Motorola serii GP. Na końcu pozostaje już tylko ubezpieczenie pojazdu, uwzględnienie w budżecie rocznych kosztów eksploatacji i wysłanie pracowników na stosowny kurs prawa jazdy.

	Cena brutto
Motocykl – Honda Transalp	25 900 zł
Kask i ubiór	2 500 zł
Ubezpieczenie OC – InterRisk (Cigna)	653 zł
Łączność – Motorola GP340 z mikrofonogłośnikiem	1 745 zł
Roczny koszt przeglądu	400 zł
Prawo jazdy kategorii A	900 zł

Ceny podane w tabeli są orientacyjne i mogą różnić się w zależności od wybranego rozwiązania.

PODSUMOWANIE

Czy warto zainwestować w motocykle? Tak, jeżeli naszym celem jest uzyskanie krótszych czasów dojazdu w godzinach szczytu. Decyzję należy jednak poprzedzić dokładną i dogłębną analizą. W innych przypadkach motocykl może stać się gadżetem reklamowym, a nie elementem przynoszącym rzeczywisty zysk. Jeżeli decyzja będzie pozytywna, to pozostaje mi tylko życzyć szerokich i prostych dróg oraz odrobiny wiatru we włosach.

Bartłomiej Dryja

Problemy wynikające z integracji systemów DSO z instalacjami SAP

artykuł sponsorowany

Z jakimi problemami muszą się zmierzyć projektanci i wykonawcy DSO? Dlaczego czasami odbiory są utrudnione i wydłużone w czasie? Czy takie problemy można przewidzieć odpowiednio wcześniej i zastosować jakieś uniwersalne rozwiązanie?

Aby odpowiedzieć na te pytania, należy zdać sobie sprawę, że zjawiska występujące w czasie nadawania sygnałów alarmowych i komunikatów słownych przez dźwiękowe systemy ostrzegawcze (DSO) oraz ich odbioru przez publiczność są bardzo złożone i dość skomplikowane. Jeśli tak, to należałoby się spodziewać, że ta dziedzina zostanie potraktowana poważnie i znajdzie należne jej miejsce w odnośnych normach i przepisach. Mimo znaczącego postępu w ostatnich latach pozostają jednak wciąż białe plamy, które jak najszybciej należałoby zapełnić, aby nie dochodziło do takich sytuacji, z jaką mieliśmy do czynienia chociażby w przypadku słynnego Terminalu 2. Portu Lotniczego w Warszawie.

Odbiorca

Co się składa na przekaz komunikatów słownych przez DSO? Zacznijmy może od końca, czyli od odbiorcy.

Każdy z nas posiada zmysł słuchu. Nasze uszy bezustannie pracują, zapewniając nam łączność ze światem zewnętrznym. Odbierają i analizują sygnały dźwiękowe, a po przetworzeniu wysyłają je do mózgu. Wszystko to dzieje się w zamkniętej przestrzeni zajmującej około 16 cm^3 dzięki wykorzystaniu zasad akustyki, mechaniki, hydrodynamiki, elektroniki i matematyki wyższej.

Mózg to najważniejsza część narządu słuchu. Przetwarza na dźwięk ogrom informacji otrzymywanych w postaci impulsów nerwowych. Ta zasadnicza rola mózgu wskazuje na szczególny związek między myśleniem a słyszeniem; zagadnieniem tym zajmuje się akustyka psychologiczna. Mózg umożliwia na przykład przysłuchiwanie się jednej z wielu rozmów prowadzonych w zatłoczonym pokoju. Mikrofon tego nie potrafi, toteż nagranie dokonane w takim pomieszczeniu byłoby raczej niezrozumiałe. Układ limbiczny pomaga mózgowi ocenić, które dźwięki są ważne, a które można pominąć. Dzięki tej umiejętności nawet w hałaśliwym otoczeniu człowiek potrafi właściwie zareagować na dźwięki alarmu czy informacji słownych przekazywanych przez DSO.

Odbiorca jest zatem wystarczająco przygotowany na odbiór treści rozgłaszanych przez DSO.

Środowisko akustyczne

W następnej kolejności od końca mamy do czynienia z o wiele mniej skomplikowaną materią, ale jednak stwarzającą największe problemy w zapewnieniu najważniejszego parametru jakościowego pracy DSO, jakim jest zrozumiałość mowy. Chodzi o środowisko akustyczne, w którym rozchodzą się fale dźwiękowe. Ideałem jest otwarta przestrzeń, w której fale dźwiękowe rozchodzą się od źródła we wszystkich kierunkach, nie napotykając na żadne przeszkody, od których mogłyby się odbić. Problem w tym, że przypadek taki jest nie do osiągnięcia, z wyjątkiem specjalnie skonstruowanej komory bezechowej czy też zawieszenia źródła dźwięku i słuchacza wysoko nad ziemią. W budynkach użyteczności publicznej fale dźwiękowe napotykają na swej drodze ściany, stropy, posadzki, okna, elementy wyposażenia. Odbijają się od nich i w konsekwencji do słuchacza dociera suma energii fal odbitych oraz fali bezpośredniej. W tym wypadku mamy do czynienia z polem akustycznym nazywanym polem rozproszonym. W idealnym przypadku, wspomnianym wcześniej, owo pole nazywa się polem swobodnym.

Jakie utrudnienia w prawidłowym rozumieniu mowy przetwarzanej przez DSO i emitowanej z głośników wynikają z istnienia powierzchni ograniczających nagłaśniany obszar budynku?

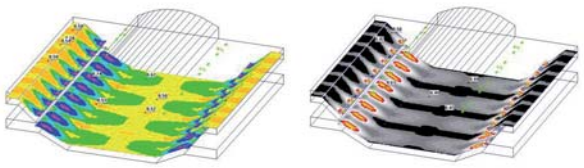
Pogłos

Pierwsze z nich to pogłos. Pogłos powstaje w wyniku wielokrotnych odbić fali dźwiękowej od powierzchni ścian, posadzki, stropu i elementów wyposażenia. W chwili, gdy źródło dźwięku przestaje generować falę dźwiękową, cisza w pomieszczeniu nie zapada od razu. Energia fal dźwiękowych zanika dopiero po jakimś czasie. Ten czas zależy od kilku czynników. Im większa jest kubatura, tym czas ten jest dłuższy. Staje się tym bardziej dokuczliwy, im twardsze są materiały użyte do wykończenia wnętrza. Do opisu ilościowego czasu pogłosu służy wzór Eyringa:

$$RT_{60} = 0{,}161 \cdot \frac{V}{S \cdot \alpha}$$

gdzie RT_{60} oznacza czas pogłosu (ang. *reverberation time*) przy spadku poziomu dźwięku o 60 dB, V to kubatura wnętrza [m3], S to suma wszystkich powierzchni ograniczających wnętrze, α to średni współczynnik pochłaniania dźwięku przez ściany, strop i posadzkę.

Tam, gdzie w grę wchodzi zapewnienie maksymalnej zrozumiałości mowy, czas ten powinien być jak najkrótszy (0,3–1,2 sekundy). Niestety, na skutek nagminnego braku współpracy architekta wnętrz ze specjalistą z zakresu akustyki środowisko akustyczne jest ostatnim elementem, jaki świadomie kształtuje się na etapie powstawania projektu. Stąd w wielu przypadkach słuchacz może zrozumieć co najwyżej pierwszą sylabę, reszta to jedynie hałas uniemożliwiający zrozumienie czegokolwiek, co powiedziano później. Czy można przewidzieć taki stan rzeczy, zanim dziarsko zabiorą się do pracy budowlańcy, a po nich fachowcy od instalacji słaboprądowych, nie bacząc przy tym wcale na to, jak mizerny będzie efekt ich często ogromnych wysiłków?



Rys. 1. (z lewej) Rzut hali sportowej z naniesionymi wartościami współczynnika zrozumiałości mowy w miejscach odsłuchu

Rys. 2. (z prawej) Zastosowanie tańszych materiałów absorpcyjnych powoduje utratę zrozumiałości mowy

Symulatory

Symulatory komputerowe pozwalają obliczyć między innymi czas pogłosu i umożliwiają modelowanie środowiska akustycznego. Należy wprowadzić niezbędne dane związane z geometrią pomieszczenia, to znaczy wymiary. Następnie dokładnie przypisać powierzchniom ograniczającym pomieszczenie współczynnik pochłaniania dźwięku i na podstawie otrzymanego wyniku czasu pogłosu RT_{60} zadecydować, czy pozostawić materiały przewidziane w projekcie architektonicznym, czy też zastąpić je innymi, o lepszych właściwościach absorpcyjnych. Na rynku są dostępne zarówno stropy akustyczne, jak i okładziny ścienne posiadające stosowne aprobaty techniczne i przebadane w akredytowanych laboratoriach. Aprobaty techniczne tych materiałów zawierają wartości współczynnika pochłaniania dźwięku dla poszczególnych pasm oktawowych. Można więc na etapie projektu zadbać o właściwe dla dobrej zrozumiałości mowy warunki akustyczne. Zdarza się jednak, że nawet wtedy, gdy wykonano symulację, warunki akustyczne pozostawiają wiele do życzenia. Przyczyny są dwie. Albo projektant przyjął złe założenia, zawyżając chłonność materiałów, albo wykonawca, szukając sposobów na obniżenie kosztów budowy, zastosował tańsze rozwiązania, grzebiąc przy tym szanse na uzyskanie przyzwoitej akustyki.

Często też wyniki symulacji komputerowych, wykonanych dla istniejących obiektów, daleko odbiegają od warunków rzeczywistych. Dzieje się tak dlatego, gdyż brak udokumentowanych wartości współczynnika absorpcji dla materiałów, jakie użyto do wykończenia danego wnętrza. Trzeba powiedzieć, że nawet niewielki wzrost czasu pogłosu RT_{60}, rzędu 0,4 sekundy, może obniżyć poziom współczynnika zrozumiałości mowy na większej części powierzchni, poniżej dopuszczalnego poziomu. W istniejących obiektach lepiej wykonać pomiar czasu pogłosu i w zależności od jego wyniku zadecydować o dalszych krokach niż zdać się na niepewny wynik symulatora. W każdym trudnym przypadku potrzebne jest jednak doświadczenie. Wyniki otrzymywane z symulatora każdorazowo należy poddać wnikliwej analizie, a to dlatego, że algorytm, zgodnie z którym dokonuje on obliczeń, przyjmuje pewne uproszczenia. Stąd wartości naniesione na wykresach mogą się różnić od rzeczywistych.

Mody własne

Oprócz pogłosu w wyniku odbić fal dźwiękowych pojawiają się również fale stojące, nazywane też modami własnymi. Pojawiają się w pomieszczeniach, w których mamy do czynienia z równoległymi powierzchniami ścian, stropu i posadzki, znajdującymi się w niewielkiej odległości od siebie. Walka z modami jest bardzo trudna, ponieważ ich występowanie wiąże się głównie z geometrią pomieszczenia. Zastosowanie materiałów dźwiękochłonnych niewiele tu pomoże, ponieważ ich efektywność absorpcji w zakresie niskich tonów, czyli tam gdzie występują mody, jest najmniejsza.

Środowisko akustyczne kształtują więc odbicia. Niemniej jednak nie jest to jedyny problem.

Hałas

Kolejny czynnik wpływający destrukcyjnie na zrozumiałość mowy to hałas. Jeśli jest nadmierny, uniemożliwia prawidłowe rozumienie mowy. Przekonano się o tym we wspomnianym wcześniej Terminalu 2. W trakcie odbioru systemu DSO zbadano współczynnik zrozumiałości mowy przy włączonym systemie oddymiającym. Okazało się, że system DSO jest bez szans. Jego najgroźniejszym konkurentem stał się system eliminujący śmiercionośny dym, a przy okazji generujący tak wysoki poziom dźwięku, że system DSO mógł mu jedynie pozazdrościć. Błąd w sztuce czy reguła? Zapewne wszyscy mieli dobre intencje. Gorzej jednak ze świadomością zależności, jakie zachodzą w sferze fal w paśmie akustycznym. Zapomniano o tym, że to, co słyszymy, stanowi superpozycję fal bezpośrednich generowanych przez wszystkie źródła dźwięku oraz wszystkich fal odbitych docierających do słuchacza. Energia tych wszystkich fal sumuje się, a jako wynik tej sumy w Terminalu 2. otrzymano potworny hałas. Zabrakło koordynacji na etapie projektowania. Zabrakło uzgodnień między branżami. System DSO i system oddymiania są jednakowo ważne. Kto jednak powinien być zainteresowany dokonaniem takich uzgodnień? Dla systemu oddymiania to bez różnicy, czy w obiekcie jest system DSO, czy też nie. Dla systemu DSO nie jest bez znaczenia, czy i jaki poziom hałasu będzie generował system oddymiający. A co na to przepisy? Owszem, jest mowa o obowiązkowym stosowaniu obu systemów w określonych obiektach. Przepisy nie mówią jednak o tym, jakie są dopuszczalne poziomy hałasu generowanego przez poszczególne systemy, które z natury rzeczy, jako produkt uboczny, dostarczają nadmiaru nikomu niepotrzebnych decybeli. Co zatem powinien zrobić wykonawca DSO, aby nie rozminąć się z celem, dla którego podjął się zadania zainstalowania i uruchomienia systemu DSO? Warto odpowiedzieć sobie na to pytanie jeszcze przed rozpoczęciem prac. Czasami trzeba samemu podjąć wysiłek i zebrać informacje od innych wykonawców, aby się zorientować, czy w ogóle istnieje jakakolwiek szansa na to, że system DSO zadziała poprawnie. W chwili odbiorów wszystkim towarzyszy najczęściej taka sama świadomość zależności występujących w akustyce, jak zawsze, czyli żadna. Dlatego wykonawca DSO może stać się przysłowiowym „chłopcem do bicia", mimo że zainstalował najlepszy system, a winę ponosi ktoś inny. Nim te sprawy zostaną uregulowane prawnie, tak jak to uczyniono w zakresie kompatybilności elektromagnetycznej, nie pozostaje nic innego, jak przejąć inicjatywę i wymusić niezbędną koordynację i uzgodnienia.

Głośniki

W dalszej kolejności, poprzez środowisko akustyczne, dochodzimy do głośników. Głośnik to przetwornik, w którym następuje konwersja sygnału elektrycznego na akustyczny. Najchętniej i najczęściej mówi się o mocy głośnika. Czy jest to faktycznie jego najważniejszy parametr, mówiący wystarczająco dużo o jakości tego urządzenia? Odpowiedź może

wiele osób rozczarować. Podawana moc nominalna informuje użytkownika, że po jej przekroczeniu głośnik ulegnie uszkodzeniu polegającym na przepaleniu cewki. O wiele ważniejsza z punktu widzenia akustyki jest jednak informacja o skuteczności głośnika, którą wyraża poziom ciśnienia dźwięku wytwarzanego przez głośnik w odległości 1 metra, po dostarczeniu do niego mocy 1 wata. Dopiero znajomość tego parametru pozwala na określenie, z jaką mocą głośnik powinien pracować, aby zapewnić wymagany poziom dźwięku w miejscu odsłuchu. Przypuśćmy, że w miejscu odsłuchu zmierzono hałas o wartości 70 dBA. Poziom dźwięku sygnału alarmowego ma być wyższy o 6 do 20 dB od szumu tła. Jeśli głośnik zamontowany jest w stropie podwieszanym na wysokości 2,5 m, to, aby spełnić ten warunek, nie można przekroczyć poziomu 90 dBA w miejscu odsłuchu znajdującym się tuż pod głośnikiem. Co to oznacza dla doboru mocy głośnika? Jeśli zastosujemy głośnik z serii MCR-SQCM produkcji Ambient System, to okazuje się, że głośnikowi wystarczy moc 0,75 W, aby spełnił on wymaganie maksimum 90 dBA w odległości 1 m. Dzieje się tak dlatego, że głośnik ten ma znakomitą skuteczność. W praktyce jednak spotykamy odwrotny trend. Projektanci z uporem godnym lepszej sprawy szafują mocą, jak Zagłoba Niderlandami. Co to oznacza dla inwestora? Załóżmy, że głośnik powinien pracować z poziomem 90 dBA w odległości 1 m, a na linii mamy ich 80. Do zasilania tej linii potrzebny jest wzmacniacz o mocy 60 W. Co się jednak dzieje, gdy projektant w swoim opracowaniu podaje, że każdy głośnik ma pobierać ze wzmacniacza 6 W? Nietrudno wyliczyć, jaką stratę finansową ponosi inwestor, płacąc za coś, czego zabroniono mu w normie. Zbędne 420 W mocy wzmacniacza kosztuje. Można też sobie wyobrazić reakcję słuchacza, który, nie spodziewając się niczego, nagle

Rys. 3. Centrala DSO ABT-Venas

usłyszy nad głową ryk sygnału alarmowego na poziomie 100 dBA. Jeszcze częściej projektanci popełniają ten błąd w przypadku podziemnych garaży. Tutaj absurdalność takiego podejścia jest jeszcze bardziej uderzająca. Trzeba zdawać sobie sprawę z tego, że w garażach podziemnych w ogóle nie występują materiały tłumiące. Twarde powierzchnie ścian stropu i posadzki wręcz bez strat odbijają falę dźwiękową pochodzącą z głośnika, powodując hałas pogłosowy – tym większy, im większa jest moc głośnika. Ponieważ głośnik dla niskich częstotliwości jest praktycznie źródłem dookolnym, to umieszczenie go na ścianie lub na stropie dodatkowo powoduje wzrost generowanego ciśnienia dźwięku o 3 dB. To tak, jakby podwoić wartość mocy dostarczanej do głośnika. Poza tym garaże są stosunkowo niskie, więc trudno znaleźć takie miejsce montażu głośnika, aby uchronić słuchacza od ogłuszającej dawki decybeli, jeśli na swoje nieszczęście znajdzie się zbyt blisko. Jak już wcześniej wspomniano, energia fal dźwiękowych sumuje się. Jeśli projektant przewidział w garażu podziemnym stanowiącym jedną strefę kilkanaście lub może nawet kilkadziesiąt głośników pracujących z pełną mocą w bezstratnym środowisku, to nietrudno zgadnąć, że huk, jaki powstanie, bez wątpienia wprawi obecnych w zdumienie. Jedynym lekarstwem w takich przypadkach jest obniżanie poziomu dźwięku, z jakim pracują głośniki, oraz zbliżenie ich do słuchaczy.

Centrala DSO

Sama centrala systemu DSO, jeśli jest dobrej jakości, tak jak ma to miejsce w przypadku systemu ABT-Venas, nie powoduje żadnych problemów. Wręcz odwrotnie. Dostarcza dodatkowych narzędzi wspomagających akustyka we właściwym zestrojeniu systemu z warunkami akustycznymi. Korektory graficzne ABT-Venas idealnie odpowiadają potrzebom kompensacji pasma przenoszenia, aby zapewnić wyrównany poziom dźwięku docierającego do słuchacza we wszystkich pasmach oktawowych składających się na pasmo mowy. Można zatem naprawić w pewnym zakresie to, co zostało zepsute przez architekta, obojętnego na wymóg zapewnienia dobrej zrozumiałości mowy, a za to chętnie serwującego pogłos, echo czy falę stojącą.

Lektor

Ostatnim elementem jest oczywiście źródło mowy, czyli lektor. W trakcie akcji ratowniczej wcieli się w tę rolę oficer straży pożarnej. Bez względu na to, kto nim będzie, jedno jest pewne. Da sobie radę!

Leszek Demidowicz
Ambient-System

ambient SYSTEM

Nowość na rynku nagłośnienia DSO

stadionów oraz hal
widowiskowo-sportowych

UWAGA

POZYTYWNA OPINIA ITB DO STOSOWANIA W DSO

Pozytywna opinia ITB
do stosowania w dźwiękowych systemach ostrzegawczych

ABT-K3012A

- idealne do obiektów wielkokubaturowych
- rewelacyjnie pracują na stadionie Lechii Gdańsk
- dalekiego zasięgu
- najwyższa jakość dźwięku bez żadnych kompromisów
- odporne na warunki atmosferyczne
- do instalacji niskoomowych oraz 100V
- przystosowane do łatwego montażu

ABT-K400 ABT-K800 ABT-K1200

- idealne do obiektów wielkokubaturowych
- wysokosprawne
- najwyższa jakość dźwięku bez żadnych kompromisów
- minimalne zniekształcenie fazowe dzięki zastosowaniu głośników koaksjalnych
- odporne na warunki atmosferyczne
- do instalacji niskoomowych oraz 100V
- przystosowane do łatwego montażu

NOWA JAKOŚĆ DŹWIĘKU NA POLSKICH STADIONACH

AMBIENT SYSTEM Sp. z o.o.
ul. Sucha 25, 80-531 Gdańsk, Polska, tel./fax: +48 58 345 51 95; 344 45 95, ambient@ambientsystem.pl, www.ambientsystem.pl

Telewizja IP z JVC Professional

Od kilku lat na rynku systemów telewizji dozorowej obserwujemy trend związany z popularyzacją rozwiązań CCTV bazujących na protokole IP. JVC jako jedna z dwóch pierwszych firm na świecie już w 1999 roku wprowadziła do sprzedaży pierwszy model kamery IP. Zalety związane z IP jako pierwsi dostrzegli wszyscy, którzy związani byli z systemami monitoringu miast. Łatwość przesyłu sygnału drogą radiową i związana z tym redukcja kosztów bardzo szybko spowodowały popularyzację takiego rozwiązania. Zaczęło powstawać coraz więcej instalacji w wielu miastach. Okazało się, że niedostępny i drogi monitoring może zawitać w mniej zamożnych lokalizacjach. Obecnie cena kamery obrotowej analogowej oraz obrotowej IP jest praktycznie identyczna. Sytuacja zmienia się jednak, gdy mówimy o kosztach kamer stacjonarnych. Tutaj widać znaczącą różnicę. Kamera IP jest wciąż wyraźnie droższa. Tak więc powstaje pytanie, czy są argumenty, niekoniecznie finansowe, za tym, aby budować systemy bazujące na kamerach IP (wyłączając wcześniej wspomniany monitoring miast)?

Okablowanie

Pierwszą rzeczą, która odróżnia system IP od analogowego, jest medium. W przypadku systemów analogowych wykorzystujemy kabel koncentryczny i złącza BNC. W przypadku analogowych kamer obrotowych potrzebować będziemy kabla, za pomocą którego prześlemy sterowanie. Dodatkowo musimy jeszcze pomyśleć o zasilaniu. W przypadku kamer sieciowych zamiast trzech kabli możemy użyć jednego – skrętki. Za pomocą takiego kabla możemy przesłać obraz, sygnały sterowania oraz zasilić kamerę poprzez przełącznik (ang. *switch*) z zasilaniem POE, czyli poprzez Ethernet (ang. *Power over Ethernet*). W tym miejscu warto zwrócić uwagę na to, że JVC w ostatnim czasie, jako pierwsza firma na rynku, wprowadziła do produkcji kamery obrotowe zasilane w ten sposób. Kamera o symbolu VN-V685 oferuje 27-krotne zbliżenie optyczne. Wyposażona jest w funkcje autotrackingu oraz stabilizacji obrazu. Możliwość zasilania kamery obrotowej za pomocą skrętki uzyskano dzięki użyciu nowoczesnego rozwiązania Direct Drive. Direct Drive to mechanizm, który bez użycia pasków i przekładni powoduje ruch głowicy. Dodatkowe korzyści z zastosowania mechanizmu to przede wszystkim szybki obrót, cicha praca oraz wysoka bezawaryjność.

Rejestracja

W przypadku systemów analogowych do dyspozycji mamy gotowe rejestratory lub też systemy kart bazujące na komputerach klasy PC. W przypadku rozwiązań IP wybór jest zdecydowanie większy. Możemy użyć gotowych rejestratorów IP lub oprogramowania zainstalowanego na komputerze. To drugie rozwiązanie jest o tyle ciekawe, że różni producenci oprogramowania oferują inteligentne rozwiązania pozwalające np. na rozpoznawanie twarzy, numerów tablic rejestracyjnych samochodów, wagonów. Przykładem jest choćby firma Axxon, która oferuje bardzo zaawansowany system rejestracji wykorzystujący kompresję Motion Wavelet. System ten można rozbudowywać o dodatkowe inteligentne funkcje. Oprócz tego jest on w pełni integrowalny z systemami bezpieczeństwa – SKD, SSWiN, SSP.

Rys. 1 Schemat systemu telewizji przemysłowej IP – do switcha biegnie jeden kabel przesyłający obraz z 3 kamer.

Rys 2.
Powyżej: *Zrzuty ekranowe darmowego oprogramowania JVC do obsługi kamer sieciowych.*
Z lewej, poniżej: *Zastosowanie kamer megapikselowych pozwala na uzyskanie szczegółowego obrazu z bardzo szerokiej sceny.*

W przypadku rejestracji obrazu z kamer IP wspomnieć należy również o możliwości zastosowania darmowego systemu rejestracji kamer JVC VN-RS800U. Jest to oprogramowanie, które pozwala na rejestrację obrazu nawet z 32 kamer IP. Oferuje nagrywanie w trybie ciągłym lub alarmowym w rozdzielczości maks. 1280x960. Liczba nagrywanych klatek zależna jest od użytego serwera. Oprogramowanie ma bardzo intuicyjny interfejs, przez co jest łatwe w obsłudze nawet dla osób nie na co dzień mających styczność z systemami telewizji dozorowej.

Rozdzielczość

Rozdzielczość to najmocniejsza strona kamer IP w stosunku do kamer analogowych. Można powiedzieć, że systemy IP wprowadziły nowe, dużo wyższe rozdzielczości. To z kolei daje nowe możliwości związane z obróbką obrazu. Przykładem niech będzie odczytywanie tablic rejestracyjnych bądź rozpoznawanie twarzy. Dodatkowo należy wspomnieć o progresywnym skanowaniu obrazu. W kamerach analogowych mieliśmy do czynienia ze skanowaniem międzyliniowym (z przeplotem). W kamerach IP występuje skanowanie progresywne, co również ma niewątpliwy wpływ na jakość obrazu. Dzięki temu porównanie obrazu z kamer analogowych i IP o tej samej rozdzielczości zdecydowanie wypada na plus dla urządzeń IP. Jeśli mowa o rozdzielczości, nie sposób nie wspomnieć o kamerach megapikselowych. Testy, które przeprowadziliśmy, pokazują, że cztery kamery o rozdzielczości 540 TVL mogą być bez obaw zastąpione jedną kamerą o rozdzielczości 1,3 megapiksela (mowa o dużych, otwartych powierzchniach typu parkingi, hale, centra handlowe). Co więcej – obraz z jednej kamery IP jest w stanie pokazać więcej szczegółów niż obraz z czterech kamer analogowych!

Podsumowanie

Powyżej wymieniliśmy korzyści związane ze stosowania systemów IP. Niewątpliwie są one duże. Można jednak zadać pytanie, czy te korzyści wpływają na cenę systemu? Odpowiedź jest następująca – wszystko zależy od rodzaju instalacji, miejsca oraz wielkości systemu. Pragniemy zwrócić Państwa uwagę na to, że budując systemy w otwartych, rozległych pomieszczeniach lub na parkingach, kamery analogowe możemy zastępować kamerami megapikselowymi. Z kosztowego punktu widzenia jest to jak najbardziej uzasadnione. Zamiast czterech kamer instalujemy jedną. Oszczędzamy w ten sposób na kablach, instalacji i obiektywach. Dodatkowe korzyści finansowe możemy uzyskać, stosując darmowe oprogramowanie JVC.

Jak wynika z powyższego, z drogiej telewizji IP przechodzimy powoli do takiej, która jest w stanie konkurować cenowo z tańszymi dotychczas systemami analogowymi, oferując zdecydowanie więcej funkcji. Warto o tym pamiętać, gdyż oznacza to, że będzie ona coraz bardziej popularna nie tylko w monitoringu miast, ale również w mniejszych instalacjach.

Łukasz Klepacki
Radioton

artykuł sponsorowany

Ustawa o bezpieczeństwie imprez masowych w praktyce

Zgodnie z uwarunkowaniami prawnymi obowiązującymi na terytorium Polski wszelkie obiekty, w których organizowane są imprezy określane jako masowe, muszą spełniać pewne wymagania formalne, precyzowane przez „Rozporządzenie w sprawie sposobu utrwalania przebiegu imprez masowych oraz minimalnych wymagań technicznych dla urządzeń rejestrujących obraz i dźwięk" z dnia 28 października 2004 r. Rozporządzenie jest datowane na rok 2004, ale opiera się na art. 15 ust. 8 „Ustawy z dnia 22 sierpnia 1997 r. o bezpieczeństwie imprez masowych". Innymi słowy stan techniki, który decydował o treści rozporządzenia, odnosi się do produktów mających obecnie minimum 11 lat. Nikomu nie trzeba tłumaczyć, jak w tym czasie zmieniła się technologia wszystkiego, co jest związane z elektroniką, a z systemami telewizji dozorowej w szczególności

Dość namacalnym przykładem ilustrującym tę sytuację jest wymóg, by obserwowany obiekt zajmował pewien procent wysokości kadru telewizyjnego. Jak ma się to do możliwości stosowania kamer megapikselowych? Czy nadal w celach identyfikacyjnych sylwetka ludzka powinna być ujmowana w tak zwanym planie amerykańskim, czyli od czubka głowy do połowy nóg? Jeśli utrzymamy ten wymóg w mocy, na obrazie z kamery megapikselowej będzie można zobaczyć nie tylko, jak wygląda identyfikowana osoba, ale także to, jak układają się najcieńsze sploty wełny w jej swetrze, a chyba nie o to chodzi służbom ochrony.

Innym problemem jest dobór sprzętu dopuszczonego do użytku w systemach monitoringu imprez masowych. Jak stwierdzić zgodność parametrów nowoczesnej kamery cyfrowej z wymaganiami rozporządzenia, gdy określa ono rozdzielczość obrazu w liniach telewizyjnych, czyli zgodnie z metodą typową dla standardu telewizji analogowej? Dla większości kamer cyfrowych taki parametr w ogóle nie jest specyfikowany, niektórzy producenci podają jedynie wyrażoną w liniach telewizyjnych rozdzielczość odnoszącą się do wyjścia analogowego, stosowanego wyłącznie do celów serwisowych, która przeważnie jest niższa od faktycznej rozdzielczości danej kamery. Jest to szczególnie widoczne w przypadku kamer megapikselowych, gdzie ta dysproporcja jest naprawdę duża.

W praktyce spotyka się przypadki, w których firmy instalujące systemy monitoringu wizyjnego muszą przedstawiać zaświadczenia, z których wynika, że obrazy pochodzące z oferowanych kamer cyfrowych zapewniają rozdzielczość obrazu lepszą niż 400 linii telewizyjnych. By takie zaświadczenie było wiarygodne, musi ono pochodzić od producenta, a ten nie jest skłonny do podpisywania jakichkolwiek oficjalnych dokumentów, proponując w zamian karty katalogowe swoich wyrobów. Kart katalogowych, w których nie ma informacji na temat rozdzielczości wyrażonej w liniach telewizyjnych, nie honoruje komisja przetargowa i koło się zamyka.

Jednakże prawdziwe problemy pojawiają się przy próbie spełnienia wymagań dotyczących rejestracji dźwięku, określonych w paragrafie 7 rozporządzenia:

1) „Utrwalony dźwięk powinien umożliwić identyfikację haseł, okrzyków i zachowań uczestników imprezy masowej w określonych strefach obiektu lub terenu, na którym odbywa się impreza masowa.
2) Urządzenia rejestrujące dźwięk powinny zapewniać możliwość rejestracji sygnału akustycznego w paśmie częstotliwości od 300 Hz do 6000 Hz przy minimalnej dynamice 50 dB".

Jeśli chciałoby się poważnie potraktować to, co wynika z punktu pierwszego, należałoby zbierać informację dźwiękową z obszaru obserwowanego przez kamery, odległego od miejsca ich instalacji nierzadko o pojedyncze setki metrów, tymczasem większość projektantów umieszcza mikrofony na tych samych wysięgnikach, na których mocowane są kamery. Są to przeważnie mikrofony o charakterystyce dookolnej, reagujące na dźwięki pochodzące z ich najbliższego otoczenia. Ma to sens tylko dlatego, że spełnia wymogi rozporządzenia, poza tym nie służy do niczego innego.

Jakie jest wyjście z tej sytuacji? Można stosować mikrofony kierunkowe, obracające się wraz z kamerami, ale jest to możliwe wyłącznie w przypadku użycia klasycznych głowic PTZ, poza tym wiąże się ze znacznymi kosztami. Można rozmieścić mikrofony w punktach objętych dozorem wizyjnym, ale trzeba dysponować odpowiednim sprzętem i oprogramowaniem, tymczasem w większości już istniejących i niestety także nowo projektowanych instalacji stosuje się najtańsze i najprostsze rozwiązania analogowe rodem z czasów, gdy jedyną legalną imprezą masową mógł być tylko pochód pierwszomajowy.

Jak na ironię, opinia osób odpowiedzialnych za bezpieczeństwo imprez masowych, dotycząca przydatności zapisu dźwięku do celów dowodowych, jest łagodnie mówiąc krytyczna, tymczasem przymus realizacji wymogów rozporządzenia pociąga za sobą znaczne komplikacje, rzutujące na budowę całego systemu, nie tylko jego części fonicznej.

Pierwsza Liga w systemach monitoringu wizyjnego.

Sony and IPELA are registered trademarks of the Sony Corporation, Japan.

SONY

www.sonybiz.net/nvm

Kamery CCTV IP, rejestratory cyfrowe, obudowy i akcesoria, oprogramowanie do monitoringu, serwisy wizyjne.

By poznać szczegóły skontaktuj się z firmą ALTRAM – autoryzowanym dystrybutorem Sony.

ALTRAM tel. +48 22 847 5505 altram@altram.com.pl www.altram.com.pl.

IPELA

W większości krajów Europy wymóg taki w ogóle nie istnieje. W związku z tym systemy monitoringu są znacznie prostsze w konstrukcji, a także tańsze i łatwiejsze do optymalizacji.

Trudno polemizować z treścią obowiązującego rozporządzenia, wymogi prawne muszą być uszanowane, jednakże nie wiadomo, kto i dlaczego zadecydował, by jako górną częstotliwość graniczną toru fonicznego przyjęto akurat 6 kHz. Jedno jest pewne – wymagań tych nie spełniają urządzenia wykorzystujące modulację G.711 z algorytmem A-law, w których parametr ten jest równy 4 kHz. Poprawa jakości dźwięku wynikająca z podwyższenia częstotliwości granicznej o mniej niż oktawę jest niewielka, ale konsekwencje praktyczne są bardzo poważne.

Różni producenci różnie radzą sobie z tym problemem. W przypadku kamer firmy Sony, fabrycznie wyposażonych w dwukierunkowy, cyfrowy kanał transmisji dźwięku, wykorzystywany jest kodek G.711 nie spełniający wymogów rozporządzenia. W związku z tym firma Sony zdecydowała się na zastosowanie zewnętrznych serwerów dźwiękowych, będących niezależnymi hostami, rozpoznawanymi w sieci na podstawie własnych adresów IP. Strumień danych generowanych przez te serwery integruje się z danymi wizyjnymi pochodzącymi z kamer na poziomie oprogramowania Sony Real Shot Manager, zachowując przy tym pełną synchronizację czasową. W ten sposób całość tworzy spójny logicznie system monitoringu, który spełnia wymagania rozporządzenia. W przypadku wykorzystania materiałów archiwalnych do celów dowodowych nie jest konieczne posiadanie licencji na pakiet Sony Real Shot Manager – wystarczy posłużyć się prostym, darmowym odtwarzaczem Ipela Media File Player o niskich wymaganiach sprzętowych, dostępnym na stronach WWW dystrybutorów sprzętu firmy Sony.

Istotną zaletą takiego rozwiązania jest brak wstępnego przyporządkowania strumieni fonicznych i wizyjnych, co w praktyce oznacza możliwość odsłuchu dźwięków pochodzących z dowolnych obszarów obiektu i powiązanie ich z obrazami faktycznie obserwowanymi przez kamery. Ma to szczególnie istotne znaczenie dla spójności zapisywanego materiału, jeśli weźmie się pod uwagę masowe stosowanie głowic obrotowych i obiektywów długoogniskowych. Poza tym wzajemne przyporządkowanie obrazu i dźwięku może być realizowane zarówno na bieżąco, w czasie trwania imprezy, jak i później, po jej zakończeniu, na materiale pochodzącym z rejestracji, co jest szczególnie dogodną cechą, gdyż wielokrotnie, w trakcie trwania zajść o charakterze chuligańskim, nie ma czasu na analizowanie, które fragmenty zapisu okażą się później istotne, a które zbędne.

Innym przykładem prób sprostania wymogom rozporządzenia może być działalność firmy, która do niedawna wykorzystywała w swoich systemach monitoringu imprez masowych pewien typ serwerów wizyjnych. Serwery te, poza swoją podstawową funkcją przetwarzania analogowych sygnałów wizyjnych w strumienie danych cyfrowych, kodowały także sygnały foniczne. Było to typowe rozwiązanie techniczne, stosowane w hybrydowych systemach monitoringu, którymi od wielu lat dysponowała ta firma. Kodowanie dźwięku odbywało się z zachowaniem wysokiej jakości, odpowiadającej kompresji MPEG-2 stosowanej przy produkcji komercyjnych płyt DVD. Określenie „do niedawna" dobrze oddaje sytuację, gdyż produkcja tego typu serwerów została wstrzymana i dotychczasowa koncepcja budowy systemów monitoringu nie mogła być dalej powielana. Od pewnego czasu żadne inne urządzenia sieciowe dostępne w ofercie tej firmy nie są w stanie kodować dźwięku z jakością wymaganą przez rozporządzenie, żadne za wyjątkiem jednego typu rejestratora…

I tu pojawiają się kolejne komplikacje. Wspomniany wyżej rejestrator jest urządzeniem przeznaczonym do pracy w popularnych niegdyś systemach hybrydowych i jako taki posiada pewną liczbę wejść analogowych, które mogą być wykorzystane zarówno do wprowadzania sygnałów wizyjnych, jak i fonicznych. Aby do tego rejestratora wprowadzić jakikolwiek sygnał foniczny, konieczne jest jego bezpośrednie powiązanie z analogowym sygnałem wizyjnym, co z kolei zmusza do stosowania analogowych kamer telewizyjnych. Wprowadzenie strumienia danych fonicznych metodą cyfrową nie jest w ogóle możliwe.

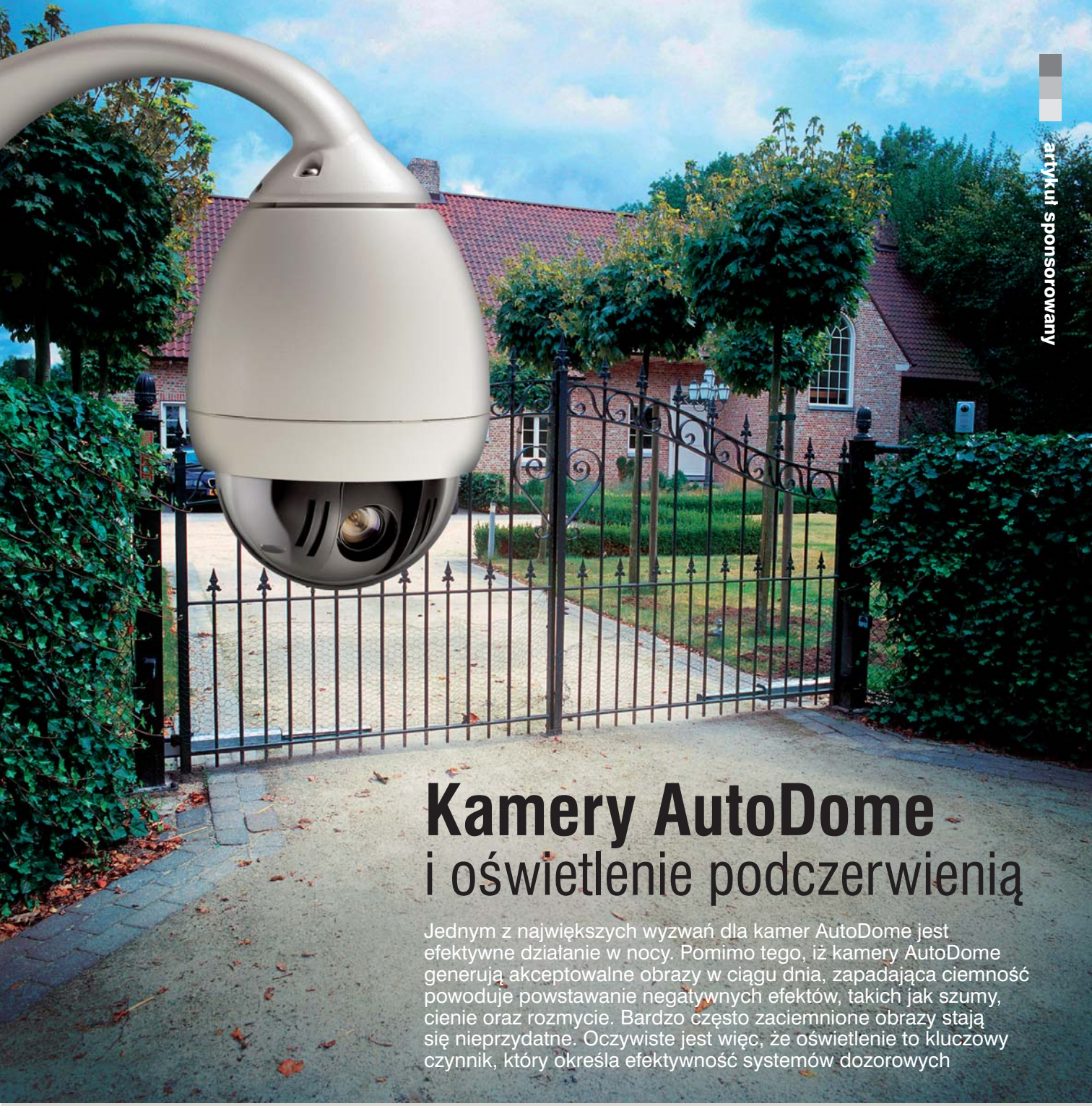
Tak więc, w chwili obecnej, chcąc zastosować urządzenia tej niewymienionej z nazwy firmy i jednocześnie spełnić wymagania rozporządzenia, trzeba użyć tylu kamer analogowych, ile mikrofonów chce się podłączyć do rejestratora. Analogowe sygnały foniczne muszą być transmitowane metodami kablowymi na długich odcinkach, co będzie wiązać się z pogorszeniem stosunku sygnału do szumu, a rozporządzenie jednoznacznie określa ten parametr jako minimum 50 dB.

Z formalnego punktu widzenia takie rozwiązanie spełnia wymagania rozporządzenia, jednakże, biorąc pod uwagę zaznaczone na wstępie tego artykułu jedenastoletnie opóźnienie w pracach legislacyjnych, nie bardzo jest się czym chwalić. Z punktu widzenia inwestora, czyli na przykład klubu sportowego będącego administratorem stadionu, rozwiązanie takie pozwala na szybkie rozpoczęcie organizacji rozgrywek, jednakże w perspektywie zaledwie kilku lat oznacza także konieczność gruntownej modernizacji systemu. Modernizacja pociągnie za sobą bardzo znaczne koszty, gdyż wszystkie urządzenia analogowe i hybrydowe powędrują do śmietnika i będą musiały być zastąpione sprzętem współczesnym, a to oznacza w przybliżeniu 50% wartości całej inwestycji. Jak na ironię, w części opisowej projektów spotyka się stwierdzenia w stylu „(...) gdy na rynku pojawią się odpowiednie urządzenia, możliwa będzie wymiana dotychczas zastosowanych na nowe (...)", co oznacza, że sami projektanci już teraz zdają sobie sprawę z wadliwości proponowanych rozwiązań.

Ponadto w cytowanym stwierdzeniu tkwi fałsz, gdyż odpowiednie urządzenia już istnieją i są dostępne na rynku, tylko trzeba chcieć ich użyć, a nie trzymać się utartych, „wypróbowanych" rozwiązań, które faktycznie są realizowane po raz pierwszy i jedyny, z braku możliwości dalszego powielania tych faktycznie wypróbowanych. No cóż, wszystko jest w porządku, bo wymagania rozporządzenia są spełnione, tyle że większość inwestorów nie do końca zdaje sobie sprawę z konsekwencji tego typu działań.

Tak więc rozporządzenie, które miało normalizować sytuację i zmuszać zarówno projektantów, jak i inwestorów do stosowania skutecznych rozwiązań technicznych, obraca się przeciwko nim, zmuszając do realizacji absurdalnych nakazów i jednocześnie skutecznie eliminując z rynku wszelkie nowatorskie pomysły. Jedyne, co pozostaje, to nadzieja, że zapowiadana od jakiegoś czasu nowelizacja rozporządzenia wyeliminuje te nonsensy i nie zastąpi ich nowymi.

ANDRZEJ WALCZYK



Kamery AutoDome i oświetlenie podczerwienią

Jednym z największych wyzwań dla kamer AutoDome jest efektywne działanie w nocy. Pomimo tego, iż kamery AutoDome generują akceptowalne obrazy w ciągu dnia, zapadająca ciemność powoduje powstawanie negatywnych efektów, takich jak szumy, cienie oraz rozmycie. Bardzo często zaciemnione obrazy stają się nieprzydatne. Oczywiste jest więc, że oświetlenie to kluczowy czynnik, który określa efektywność systemów dozorowych

Oświetlenie podczerwienią

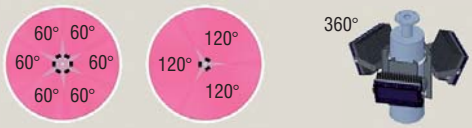
Oświetlenie podczerwienią (IR) jest od wielu lat stosowane do rozwiązywania problemów z dozorem wizyjnym w ciemności oraz przy słabym oświetleniu. Zaprojektowane specjalnie do zastosowań dozorowych oświetlenie podczerwienią jest istotnym elementem systemu, wykorzystywanym przez kamery do generowania wyraźnych obrazów w złych warunkach oświetleniowych lub przy całkowitym braku oświetlenia. Oświetlenie podczerwienią daje dodatkową korzyść – jest niewidoczne dla oka ludzkiego.

Prawidłowe dobranie oświetlenia podczerwienią jest relatywnie proste. Kluczowymi czynnikami są: długość fali, układ wiązki, zasięg oświetlenia. Ponadto nie każde światło jest generowane w ten sam sposób, dlatego ważne jest, aby wybrać właściwy jego rodzaj w zależności od zastosowania. Na przykład oświetlacze podczerwieni Black Diamond firmy Bosch generują jednolite oświetlenie, eliminując jasne punkty oraz niedoświetlone obszary znajdujące się w zasięgu wiązki światła.

W większości zastosowań istnieją trzy sposoby wykorzystania oświetlenia podczerwienią.

Sposób 1 – Dookolny obszar oświetlenia 360°

Najbardziej wszechstronnym podejściem jest instalacja oświetlenia podczerwienią o pokryciu 360°, która gwarantuje, że światło będzie dostępne z każdej strony wokół kamery, co zmniejsza ryzyko pominięcia przez kamerę ważnych zdarzeń rozgrywających się w ciemnościach.



Rys. 1. Sposob 1 – Dookolny obszar oświetlenia 360°

Konwencjonalne oświetlacze podczerwieni były wyzwaniem dla instalatorów systemów dozorowych, ponieważ do osiągnięcia pokrycia 360° wymagały użycia przynajmniej sześciu urządzeń. Jednakże nowa, obsypana nagrodami technologia Black Diamond, wykorzystująca soczewki mikrorefrakcyjne, pozwala uzyskać za pomocą jednego oświetlacza pole pokrycia o kącie do 120°. W związku z tym trzy oświetlacze podczerwieni Black Diamond osiągają pełne pole pokrycia 360°.

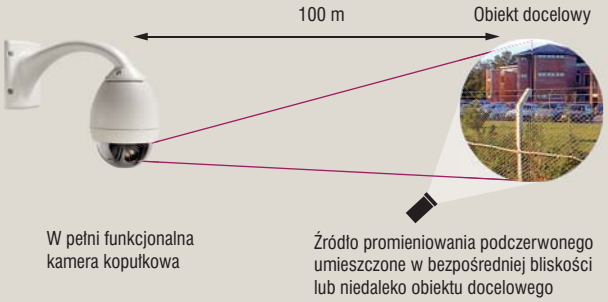
Sposób 2 – Oświetlenie określonego obiektu docelowego

Alternatywne względem powyższego rozwiązanie można uzyskać przez zastosowanie oświetlenia określonego obiektu docelowego. Jest to metoda oświetlenia sceny i jej otoczenia w taki sposób, aby oświetlone były tylko określone obszary ryzyka zamiast całej sceny obserwowanej przez kamerę. Technologia polegająca m.in. na strategicznym rozmieszczeniu oświetlaczy podczerwieni w celu oświetlenia obiektów docelowych bazuje na doborze właściwego oświetlenia do obszarów ryzyka w obserwowanym otoczeniu. Mogą być to bramy, wejścia i wyjścia, drogi i chodniki, gdzie istnieje duże prawdopodobieństwo pojawienia się intruzów. Podczas pełnego obrotu kamery (360°) jedynie dwa lub trzy obiekty docelowe mogą być obserwowane przy oświetleniu podczerwienią. Oświetlacze podczerwieni mogą być zamocowane na maszcie kamery i wokół niego w celu ciągłego oświetlania obiektów docelowych, co umożliwia efektywne monitorowanie kluczowych obszarów sceny przez kamerę.

Rys. 2. Sposob 2 – Oświetlenie określonego obiektu docelowego

Sposób 3 – Oświetlenie obszaru lokalnego

Niektóre warunki środowiskowe mogą wymagać umieszczenia oświetlacza podczerwieni z dala od kamery. Na przykład w miejscu instalacji kamery mogą istnieć ograniczenia związane z zasilaniem, które stwarzają potrzebę poprowadzenia dodatkowego okablowania. Pomiędzy kamerą i docelowym obszarem dozoru może także istnieć duża odległość, co wymaga więcej energii do oświetlenia oddalonego obszaru.



Rys. 3. Sposob 3 – Oświetlenie określonego obiektu lokalnego

W takich sytuacjach należy rozważyć instalację oświetlacza podczerwieni ponad określonym obiektem docelowym lub w jego pobliżu. W celu uzyskania najlepszych rezultatów należy prawidłowo dobrać kąt kamery w stosunku do typu oświetlenia podczerwienią oraz rozmieścić oświetlacze tak, aby zredukować cienie na obiekcie docelowym.

Sposób 4 – Kamera ze zintegrowanym oświetleniem podczerwienią – MIC1-400

Wbudowanie oświetlenia podczerwienią bezpośrednio w mechanizm uchylno-obrotowy sprawia, że wiązka podąża za kierunkiem obserwacji kamery. Technologia ta ma tę zaletę, że oświetlenie podczerwienią jest dostępne dla kamery niezależnie od jej położenia. Zasadniczo technologia osiąga

Rys. 4. Sposob 4 – Kamera ze zintegrowanym oświetleniem podczerwienią – MIC1–400

rzeczywiste pokrycie 360° bez strat światła w obszarach nieoświetlonych. Zważywszy na to, że technologia jest dostępna przy użyciu konwencjonalnych mechanizmów uchylno-obrotowych, kamery kopułkowe MIC1-400 z funkcją obrotu, pochylenia i zoomu gwarantują szybsze działanie, mając jednocześnie znacznie mniejsze obudowy.

Integracja ramek

Niektóre kamery kopułkowe używają technologii integracji ramek w celu uzyskania wyraźnych obrazów w ciemnych scenach. Ponieważ technologia ta zwykle powoduje spowolnienie prędkości migawki oraz łączenie ramek, jest akcep-

Rys. 5. Integracja ramek

towana tylko w ograniczonej liczbie zastosowań. Integracja ramek generalnie nie sprawdza się przy obrazowaniu poruszających się obiektów, gdyż w takim przypadku powoduje rozmycie obrazu oraz utratę szczegółów. Jeśli na przykład intruz porusza się podczas wykonywania „trasy" przez kamerę, zostanie on zarejestrowany w postaci rozmazanej plamy, a ważne informacje i szczegóły zostaną utracone. W rezultacie w nagraniu z systemu dozorowego będą znajdować się duże i potencjalnie brzemienne w skutkach przerwy.

Problem rozmycia ruchu spowodowany integracją ramek może być w łatwy sposób rozwiązany przez zapewnienie lepszego oświetlenia. Używając oświetlenia podczerwienią, kamera określa, czy oświetlenie sceny jest wystarczające. Jeśli jest, nie włącza trybu integracji ramek. Ruch w nocy przy wystarczającym oświetleniu podczerwienią jest odbierany tak samo, jak gdyby był rejestrowany w dzień: jest wyraźny, a krytyczne szczegóły są doskonale widoczne.

Podczerwień i wizyjna detekcja ruchu (*Video Motion Detection* – VMD)

Oprogramowanie do analizy obrazu, tak jak każde inne, wymaga aktualnych danych, aby działać prawidłowo. Bez aktualnych danych dla algorytmów, które mają być przetwarzane, nawet najbardziej zaawansowane oprogramowanie do analizy obrazu nie sprawdzi się. Konieczność zapewnienia odpowiednich danych odzwierciedla jedno z najstarszych praw informatycznych: *Garbage In, Garbage Out* (śmieci na wejściu, śmieci na wyjściu).

Technologia oświetlaczy podczerwieni umożliwia analizę obrazu w nocy i eliminuje źle oświetlone, zaszumione obrazy powstające zwykle przy niskim poziomie oświetlenia. Zaszumione obrazy, które są skutkiem ubogich danych, powodują problemy w działaniu oprogramowania do analizy obrazu, co prowadzi do nieprawidłowego obrazowania (renderowania, ang. *rendering* – przyp. red.). Zastosowanie oświetlaczy podczerwieni znacznie poprawia jakość obrazów, a tym samym umożliwia uzyskanie wysokiej rozdzielczości. Obrazy te z kolei służą jako dane wejściowe, które umożliwiają prawidłowe działanie oprogramowania do analizy. Podobnie jest w przypadku innych funkcji przetwarzających obraz, stosowanych w rejestratorach cyfrowych, rejestratorach sieciowych oraz cyfrowych systemach zarządzania obrazem, które nie zdają egzaminu w nocy. Wszystkie te funkcje, m.in. wizyjna detekcja ruchu, automatyczne alarmy, eliminowanie fałszywych alarmów, wyszukiwanie ruchu w obrazie, wykrywanie włamań, zapis zdarzeń, do prawidłowej pracy wymagają obrazów o wysokim stosunku sygnał/szum, a w złych warunkach oświetleniowych działają optymalnie, kiedy są używane w połączeniu z oświetleniem podczerwienią.

Podsumowanie

Istnieją cztery główne strategie efektywnego wykorzystania oświetlenia podczerwienią z kamerami obrotowymi:

1) oświetlenie obszaru w zakresie 360°, gdy do pokrycia całego obszaru otaczającego kamerę AutoDome używanych jest kilka oświetlaczy podczerwieni;
2) oświetlenie określonego obiektu docelowego, gdy oświetlacze podczerwieni są rozmieszczone tak, aby oświetlały tylko określone obszary lub obiekty;
3) oświetlenie obszaru lokalnego, gdy oświetlacze podczerwieni są rozmieszczone w pobliżu określonych obiektów docelowych, które są monitorowane;
4) bezpośrednia integracja z kamerami obrotowymi, gdy oświetlacze podczerwieni są przymocowane bezpośrednio do kamer i poruszają się wraz z nimi.

Użycie oświetlenia podczerwienią przynosi także wymierne korzyści z punktu widzenia funkcjonalności technologii integracji ramek, wizyjnej detekcji ruchu oraz analizy obrazu.

Warto podkreślić, że każda z powyższych strategii odnosi się w tym samym stopniu do oświetlenia podczerwienią oraz do oświetlenia światłem widzialnym, które jest często wymagane w zastosowaniach, w których niezbędne jest nocne monitorowanie wizyjne w kolorze. Więcej informacji o oświetlaczach (reflektorach) światła białego znajduje się w dokumentacji produktów AEGIS White Light firmy Bosch.

BOSCH SECURITY SYSTEMS

ZSJZ

AQAP 2110:2006

Certyfikowany na zgodność z: PN - EN ISO 9001 : 2001

1993 ISTNIEJEMY OD

firma **ATLine®**

kompleksowe zabezpieczanie obiektów

MMD - SYSTEM
200 m

PRZENOŚNY SYSTEM OCHRONY ZEWNĘTRZNEJ
Z RADIOWĄ CENTRALĄ ALARMOWĄ I CYFROWYMI BATERIAMI

- zasięg: 200 metrów
- zakres temperatury: od -40 do +65 °C
- zasilanie autonomiczne z baterii: do 20dni
- okablowanie: kable w pancerzu i złączki wojskowe
- zestaw zawiera skrzynie transportowe odporne na uszkodzenia
- nominalny zasięg transmisji sygnałów i regulacji: drogą radiową od 500 do 1000 metrów
- kolor: zieleń wojskowa, pustynny piaskowy
- odporność na małe zwierzęta i warunki atmosferyczne

AN303
600 m

OCHRONA OBWODOWA OGRODZEŃ

- sterownik czyjnika wibracyjnego oraz kabel sensoryczny
- 2 strefy: do 300 metrów każda, max 600 metrów
- zakres temperatury: od -40 do +70 °C
- możliwość podsłuchu
- dwa przekaźniki bezpotencjałowe na każdą strefą (alarm, sabotaż)
- cyfrowa regulacja czułości dla każdej strefy, na płycie za pomocą przycisków
- obudowa zewnętrzna aluminiowa PI65
- odporność na małe zwierzęta i warunki atmosferyczne

MANTA
50, 80 m

ZEWNĘTRZNA MINIATUROWA BARIERA MIKROFALOWA
Z CYFROWĄ OBRÓBKĄ SYGNAŁU

- zasięg: 50, 80 metrów
- zakres temperatury: od -40 do +65 °C
- modulacja częstotliwości - 16 kanałów do wyboru
- przekaźniki bezpotencjałowe (alarm, sabotaż, uszkodzenie)
- złącze RS485 i oprogramowanie Wave-Test
- komplet RX i TX do montażu na słupku o średnicy zewnętrznej 40 mm
- odporność na małe zwierzęta i warunki atmosferyczne

Firma ATLine sp. j. K. Cichulski S. Pruski

91-845 Łódź, ul. Franciszkańska 125, tel. +48 42 657 30 80, fax +48 42 655 20 99
e-mail: info@atline.pl, handel@atline.pl, www.atline.pl

Innowacja w zabezpieczeniach

Centrala INTEGRA 128-WRL

Centrala o możliwościach INTEGRY 128, wyposażona w komunikator GSM/GPRS i technologię dwukierunkową bezprzewodowej łączności z czujkami ABAX. Rozwiązanie dające maksimum korzyści oferowanych przez technologię bezprzewodową z elastycznością i funkcjonalnością tradycyjnych systemów przewodowych.

Nowość

Złoty Medal Targów Poznańskich przyznany centrali za jej innowacyjność, wszechstronność i technologiczne zaawansowanie.

Satel®

ul. Franciszka Schuberta 79, 80-172 Gdańsk, tel.: (0 58) 320 94 00, fax: (0 58) 320 94 01
e-mail: satel@satel.pl, www.satel.pl

artykuł sponsorowany

Nowy rejestrator marki NOVUS z kompresją H.264

W magazynie *Zabezpieczenia* nr 5/2008 przedstawiłem czterokanałowy rejestrator NV-DVR1014. W tytule określiłem go jako rejestrator dla małych systemów, co jest oczywiste w kontekście tylko czterech wejść wizyjnych. W związku z tym artykułem pojawiły się jednak pytania odnośnie rejestratorów ośmio- albo szesnastokanałowych, które zastąpiłyby dotychczasowe rejestratory serii 1100 z systemem kompresji M-JPEG. I właśnie tym rejestratorom, których projekt został właśnie zakończony, chciałbym poświęcić niniejszy artykuł

Firma NOVUS ma w ofercie dwa modele rejestratora: ośmiokanałowy NV-DVR1208/DVD oraz szesnastokanałowy NV-DVR1216/DVD. Jak to zwykle bywa, różnice pomiędzy tymi modelami dotyczą tylko liczby wejść wizyjnych, alarmowych, wyświetlanych podziałów itp., natomiast zastosowane rozwiązania są identyczne.

W urządzeniach zastosowano standard kodowania sygnałów wizji H.264, który jest dziesiątą częścią standardu MPEG-4, dotychczas powszechnie wykorzystywanego w urządzeniach rejestrujących. Pierwotnie standard H.264, zapewniający relatywnie najmniejsze przepływności, przewidziany był do wykorzystania w transmisji sieciowej. Efektywność kompresji standardu H.264, większa aniżeli w przypadku innych standardów, okupiona jest jednak znacznie większym zapotrzebowaniem na moc obliczeniową rejestratora. Dlatego też często można się spotkać z rejestratorami z kompresją H.264, które pozwalają na odtwarzanie (dekodowanie) tylko pojedynczego lub co najwyżej dwóch strumieni wizji ze względu na ograniczone zasoby urządzenia. Jest to poważne ograniczenie, które nie pozwala na synchroniczne odtwarzanie strumieni w dowolnych podziałach i ich równoległą analizę. W dotychczas oferowanych rejestratorach możliwość odtwarzania w podziale była dla użytkowników systemów telewizji dozorowej oczywistością, o której nie wspomina się ani w kartach katalogowych, ani w wymaganiach przetargowych, ale ta właściwość wymaga jednak weryfikacji, gdyż nie zawsze najnowsze modele ją zapewniają. W przypadku rejestratorów NV-DVR1208(16)/DVD istnieje możliwość płynnego odtwarzania wszystkich kanałów w dowolnych podziałach.

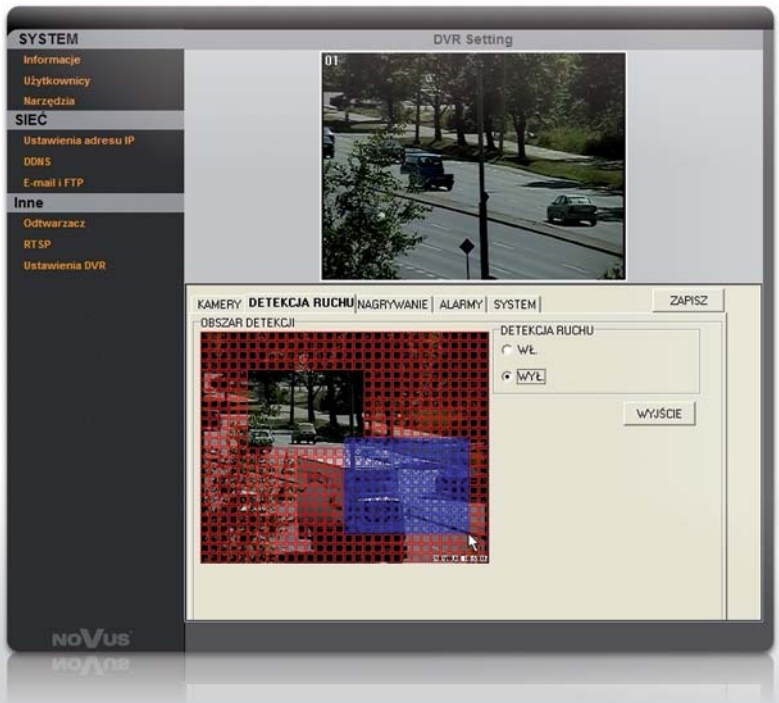
Zarejestrowane strumienie wideo mogą być odtwarzane według takich zdarzeń jak: detekcja ruchu, utrata wizji, aktywacja wejść alarmowych, utrata zasilania lub rozpoczęcie nagrywania. Dodatkowo można wybrać konkretną datę i czas lub posłużyć się graficznym kalendarzem. W rejestratorze zaimplementowano również funkcję synchronizacji czasu systemowego z serwerem czasu. W przypadku cofnięcia czasu systemowego oba zarejestrowane segmenty zostaną zachowane.

W urządzeniu można zainstalować do dwóch dysków twardych o pojemności 1TB każdy. Są to dyski SATA z kontrolerami transmisji szeregowej. Nie są tu stosowane konwertery standardu IDE, co pozwala w pełni wykorzystać zalety transmisji szeregowej.

Rejestrator rejestruje do 200 obrazów/s o rozdzielczości 360x288 lub 100 obrazów/s w półobrazach. Ustawienia prędkości zostały zindywidualizowane dla każdej kamery w ramach dostępnego całkowitego limitu prędkości nagrywania. Ustawienia te można zrealizować niezależnie dla nagrywania ciągłego oraz dla nagrywania alarmowego. Dodatkowo dla każdej kamery można niezależnie ustawić stopień kompresji, czyli jakość nagrywanego strumienia. Przejrzysty graficzny harmonogram pozwala ustawić tryb nagrywania (ciągły, alarmowy lub łączony) z dokładnością do jednej godziny dla każdego dnia tygodnia. W systemie można zdefiniować do pięciu niezależnych harmonogramów i następnie przełączać się między nimi.

Rejestratory mogą generować strumienie RTSP, które mogą być odbierane m.in. przez niektóre modele telefonów komórkowych z definiowaną jakością strumienia.

W menu rejestratora lub w menu interfejsu sieciowego można dokonać ustawień dotyczących wysyłania plików wideo w formacie *.264 na serwer FTP i (lub) pocztowy. Po wykryciu ruchu lub w momencie aktywacji wejścia alarmowego rejestrator wysyła e-mail z załączonym plikiem wideo lub eksportuje go na serwer FTP. Funkcja ta pozwala na



Rys. 1. Okno ustawień detekcji ruchu przy połączeniu zdalnym

szybki zdalny dostęp do zdarzeń alarmowych w systemie oraz uzyskanie zdalnej kopii zdarzeń alarmowych, ważnych szczególnie w przypadku utraty lub fizycznego zniszczenia rejestratora.

Rejestratory NV-DVR1208/DVD i NV-DVR1216/DVD mają możliwość kopiowania zarejestrowanych na dysku twardym danych do pamięci Flash z interfejsem USB, na płytach CD lub DVD we wbudowanej nagrywarce DVD lub poprzez sieć na dysku twardym komputera. Razem z plikiem kopii do pamięci kopiowany jest program N-Viewer1200, za pomocą którego możliwe jest przeglądanie na komputerze PC pliku kopii. Odtwarzacz posiada dodatkowo funkcję przeglądania zawartości dysków z nagraniami, wyjętych bezpośrednio z rejestratora. Jest to szczególnie ważne w przypadku konieczności przeanalizowania nagrań z dłuższego okresu, których kopiowanie byłoby procesem długotrwałym i żmudnym. Oglądane nagrania można zapisać na komputerze PC, a następnie skonwertować do pliku AVI.

Rejestrator wyróżnia się różnorodnością sposobów jego obsługi. Może być ona realizowana z poziomu przycisków na panelu czołowym, za pomocą pilota sterowania zdalnego o zasięgu do siedmiu metrów, myszy USB znajdującej się w zestawie oraz z poziomu klawiatur systemowych NV-KBD60 oraz NV-KBD30 przy użyciu protokołu Novus-D3 lub N-Control.

Rejestratory NV-DVR1208/DVD i NV-DVR1216/DVD pozwalają sterować kamerami wyposażonymi w interfejs RS485. Mogą to być zarówno kamery szybkoobrotowe serii CAMA-I, CAMA-II oraz CAMA-II mini, jak i stacjonarne z optycznym i cyfrowym zbliżeniem. Sterowanie może być realizowane z poziomu przycisków na panelu czołowym, pilota zdalnego sterowania, za pomocą myszy USB z poziomu menu ekranowego lub z poziomu przeglądarki internetowej. Sterowanie odbywa się w protokole Novus-C, Pelco-D lub dodatkowo w protokole N-Control. Rejestrator umożliwia zdefiniowanie parametrów transmisji oddzielnie dla każdej kamery, tym samym w systemie można równocześnie sterować kamerami z wykorzystaniem różnych protokołów.

Najważniejszym usprawnieniem w porównaniu do poprzednich modeli rejestratorów serii 1000 jest rozbudowa apletu sieciowego. W aplecie sieciowym została dodana zakładka „Ustawienia rejestratora", pozwalająca na zdalną zmianę ustawień rejestratora. Zmiana ustawień dotyczy wszystkich parametrów za wyjątkiem ustawień systemowych, np. czasu lub numeru ID urządzenia. Narzędzie to jest szczególnie przydatne do weryfikacji i korekcji siatki detekcji ruchu czy zmiany parametrów nagrywania i tym samym dostępnego archiwum.

W niniejszym artykule ograniczyłem się tylko do opisu najważniejszych parametrów wyróżniających rejestratory NV-DVR1208(16)/DVD spośród dotychczasowych modeli. Szczegółowe dane wymagane do konkretnych specyfikacji są podane w instrukcji obsługi i karcie katalogowej urządzenia. Dokumenty te są dostępne na stronie *http://www.novuscctv.pl*.

W celu podniesienia funkcjonalności rejestratorów rozwijana jest aplikacja sieciowa umożliwiająca równoczesny dostęp do wielu rejestratorów. Pozwoli to na zastosowanie rejestratorów w systemach rozproszonych (grupach obiektów) i obsługiwanie ich z jednego centrum obsługi. Dodatkowo trwają również prace nad aplikacją dla urządzeń mobilnych.

Patryk Gańko
Novus Security

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

NOWE rejestratory z kompresją H.264

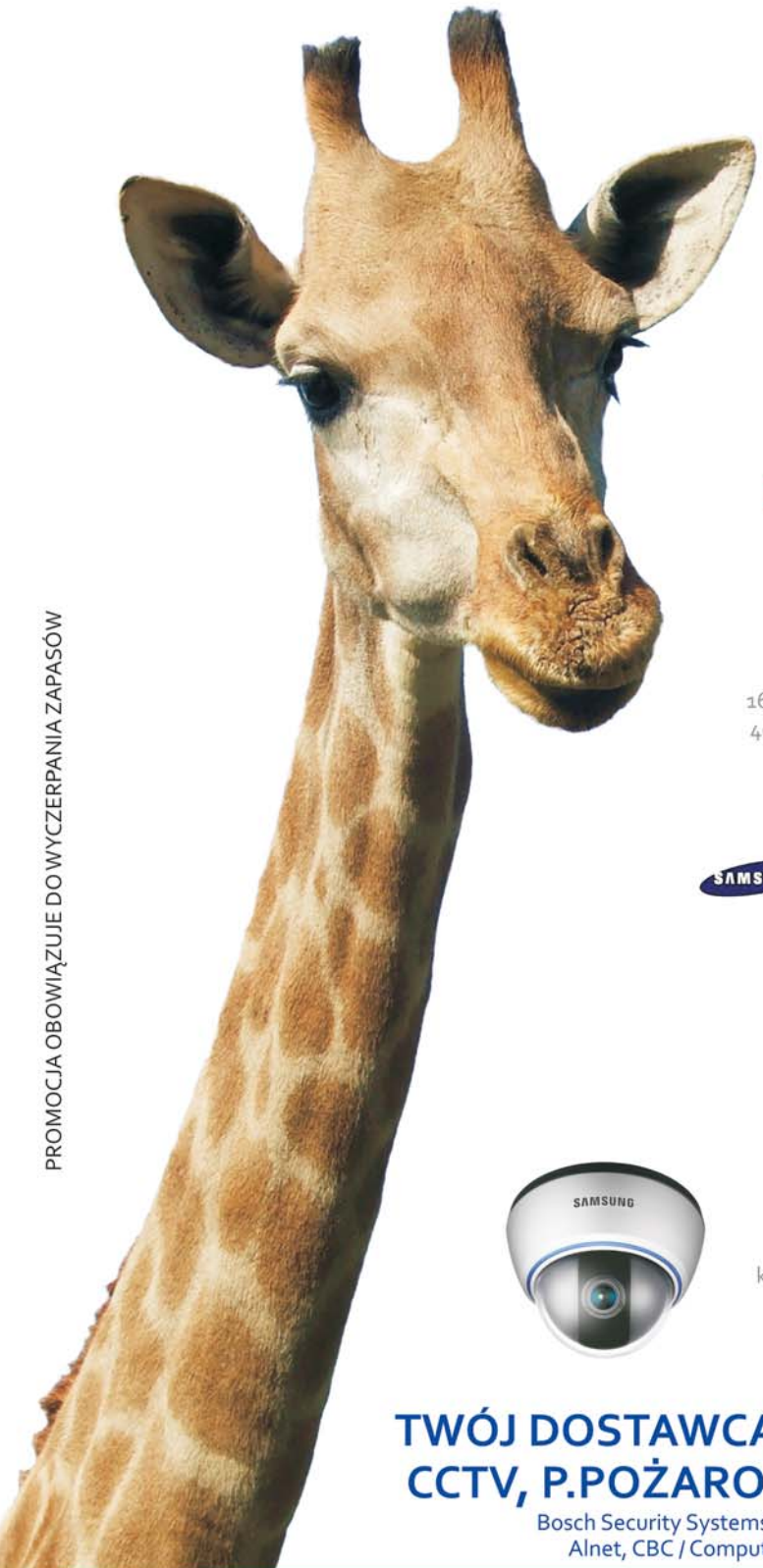
8/16-kanałowe rejestratory cyfrowe serii 1200

- tripleks: zapis, odtwarzanie i połączenie sieciowe
- prędkość nagrywania do 200 obr/s
- H.264, rozdzielczość nagrywania: 720x288, 360x288
- odtwarzanie w podziałach: pełny ekran, 4, 9, 16
- zaawansowane funkcje harmonogramu nagrywania i detekcji ruchu
- kopiowanie nagrań poprzez port USB, CD/DVD i sieć komputerową
- zmiana ustawień rejestratora przez sieć
- współpraca z klawiaturą NV-KBD60 i NV-KBD30
- wbudowana nagrywarka DVD-RW
- oprogramowanie: N-Viewer1200 do przeglądania kopii nagrań i odczytu dysków z rejestratora

Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Holding sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 541
www.aat.pl

PODAJEMY PRODUKTY Z GÓRNEJ PÓŁKI



PROMOCJA OBOWIĄZUJE DO WYCZERPANIA ZAPASÓW

CCAS 1425 LPO

SIEMENS

zewnętrzna - IP 66, dualna z filtrem IR, zoom optyczny 22-krotny 3,9 - 85,8 mm, szerokodynamiczna - WDR, 540 linii, preset wyzwalany stykiem zewnętrznym, uchwyt z kanałem kablowym, pilot w zestawie

cena detal. 1899,00 -30 % = **1329,00** netto

Divar MR, DVR 16 L-100A

BOSCH

16 wejść video, 8 wej. fonicznych, dysk 1000 GB, DVD,monitor VGA i BNC 400 kl/s - CIF, 100 kl/s - 4 CIF, oprogramowanie Control Center w zestawie

cena detal. 14726,00 - 60% = **5890,00** netto

SVR - 1645

SAMSUNG TECHWIN

16 wejść video, 4 wej. Foniczne, dysk 250 GB (max 4 dyski 750 GB), 400 kl/s - CIF, 100 kl/s - 4 CIF, DVD, monitor VGA i BNC

cena detal. 7700,00 - 40% = **4620,00** netto

SID 560

kamera dualna z filtrem IR, rozdz. 560 / 700 linii obiektyw 2,8-10 mm, AI, szerokodynamiczna WDR, zasilanie 12 / 24 V

cena detal. 859,00 - 30% = **599,00** netto

TWÓJ DOSTAWCA SYSTEMÓW ALARMOWYCH, CCTV, P.POŻAROWYCH, NAGŁOŚNIENIA, DSO

Bosch Security Systems, Siemens, Ge Security, Satel, SPS Traiding, Gorke, Alnet, CBC / Computar, Samsung, ADI Ultrak, Vidicon, Altram, Aper

euroalarm

www.euroalarm.com.pl

GORZÓW WLKP., ul. Borowskiego 34, tel. 095 73 52 102
BYDGOSZCZ, ul. Piękna 25, tel. 052 325 40 10-15
TORUŃ, ul. Kościuszki 16A, tel. 056 659 83 77
KOSZALIN, ul. Młyńska 48, tel. 094 345 83 30

Akt I
Poniedziałek, 7:59

Za chwilę się zacznie. A w weekend było tak miło... W piątkowy wieczór spotkanie ze znajomymi, impreza do późnych, a w zasadzie wczesnoporannych, godzin. W sobotę odsypianie, sprzątanie, zakupy, wieczorem odpoczynek przy szklaneczce ulubionej whisky z lodem i dobrym filmie przyniesionym z pobliskiej wypożyczalni. W niedzielę rodzinny obiad, wyjście do kina. Ech... Jak tu powrócić do cotygodniowego rytmu, skoro nawet kawa jeszcze nie wypita. Czas włączyć komputer i zerknąć, co tam nowego piszą w ulubionym portalu o wydarzeniach z ostatnich dni. Dzwoni telefon. Któż to o tej porze może chcieć już czegoś ode mnie? Przecież dopiero dwie po ósmej... Podnoszę ze zrezygnowaną, a zarazem pełną irytacji miną słuchawkę telefonu i pytam tonem bez życia, o co chodzi. Po drugiej stronie słyszę miły, pełen pogody męski głos (pewnie ten ktoś przychodzi do roboty na 7:00 i już jest po kawie, nie dając jej wypić innym!): ***– Dzień dobry! Tu Andrzej Janowski, jestem nowym administratorem. Na Twoim koncie w systemie operacyjnym zauważyłem błędy. Czy możesz się teraz wylogować i zalogować ponownie?*** Świetnie rozpoczyna mi się tydzień, nie ma co! – myślę. Nie dość, że nic nie rozumiem z tego, o co mnie ten młody człowiek pyta, to jeszcze tego by brakowało, żeby mi się problemy z komputerem zaczęły. Muszę przecież przed końcem tygodnia oddać raport ze sprawozdaniem finansowym na koniec kwartału. Akcjonariusze naszej spółki już nie mogą się doczekać jego ogłoszenia! Będzie wtedy wiadomo, czy warto inwestować w akcje firmy, czy nie. Ci, którzy tuż przed ogłoszeniem raportu zakupią dużą liczbę akcji, powinni nieźle na tym zarobić. W końcu osiągnęliśmy w tym kwartale dobry wynik. Jest się czym pochwalić! Spełniam zatem prośbę pana Andrzejka, trwa to chwilę. Na tyle długo, że mogę wziąć kilka łyków ciepłej kawy i delektować się jej smakiem. Nic tak dobrze nie smakuje w poniedziałkowy poranek, jak cudowna, kojąca nerwy kawa. W słuchawce odzywa się znajomy głos: ***– Czy udało się przeprowadzić operację?*** O jakiej operacji człowieku mówisz? Wyloguj i zaloguj? To tylko kilka czynności, a pytanie zabrzmiało tak, jakby trzeba było zoperować komuś serce! Potwierdzam od niechcenia. ***– Dziwne. Nadal pojawia się ten sam błąd. Niestety może on skutkować zablokowaniem konta użytkownika. Ale postaram się jakoś pomóc, w końcu pracujemy od niedawna razem!*** – dodaje mój rozmówca z entuzjazmem w głosie. Nie wiem skąd w nim tyle energii. Widocznie rzeczywiście dostał tę robotę całkiem niedawno i jeszcze rozpiera go chęć naprawiania świata. ***– Zróbmy może tak. Nie chcę zajmować czasu, więc sam dokonam kilku prób i sprawdzę, czy da się jakoś problemowi zaradzić. Czy mogę zatem prosić o podanie loginu i hasła? Sam sprawdzę i oddzwonię z informacją, czy udało się rozwiązać kłopot.*** Z nadzieją na to, że w końcu ten młody człowiek da mi święty spokój, a co więcej: uwolni mnie od nikomu niepotrzebnych – a na pewno nie mnie – kłopotów, dyktuję mu przez telefon magiczne słowa. Nazwa użytkownika jest stosunkowo prosta. Ale już moje hasło muszę mu przedyktować trzy razy. Z nieukrywaną dumą w głosie! Składa się z dwunastu znaków, a pośród nich są zarówno małe, jak i wielkie litery, cyfry i znaki specjalne! Nie byle co! Aż roi się w nim od „małp", „haszy" i „dolarów". W końcu zajmuję się odpowiedzialną „działką" w firmie i muszę dbać o ochronę dostępu do swojego komputera. Przechowuję na swoim pececie bardzo wrażliwe dane i niejeden chciałby do nich niepostrzeżenie dotrzeć, ale nic z tego! Złamanie hasła zajęłoby intruzowi wieki, nawet z wykorzystaniem specjalistycznych narzędzi programowych. Kiedy upewniam się, że „admin" dobrze zapisał hasło, rozłączam się. Niech każdy zajmie się swoją robotą, to może jakoś uda się dotrwać do końca tygodnia.

Po dziesięciu minutach ponownie dzwoni człowiek o miłym i ciepłym głosie z informacją, że już wszystko w porządku, życząc przy okazji miłego tygodnia w pracy. Uff! – myślę sobie, dodając kolejną tabelkę z liczbami do kwartalnego raportu – całe szczęście, że już po problemie! Mogę spokojnie popracować i na pewno zdążę na czas z wykonaniem swojego zadania.

Akt II
Piątek, 14:05

Hurra! Raport ukończony, wersja wydrukowana zaakceptowana przez szefa, plik wysłany mailem do przygotowania do publikacji. Za mną pracowity tydzień, ale było warto! Szef zadowolony, na pewno nie zapomni o nagrodzie przy najbliższej premii kwartalnej. W końcu mamy świetne wyniki finansowe, a wykonana przeze mnie praca uzyskała aprobatę już przy pierwszym czytaniu. Było tylko kilka sugestii dotyczących naniesienia drobnych poprawek redakcyjnych, ale to już małe piwo.

Po pół godzinie materiał był gotowy do wysłania! Zostały mi jeszcze prawie dwie godziny do weekendu. Mogę je teraz spędzić na słodkim lenistwie i planowaniu tego, co będę robić w weekend. Muszę dobrze odpocząć, bo w poniedziałek ważny dzień: publikacja mojego raportu. Mam zatem co świętować! Do pokoju wchodzi młody człowiek z dziwnym przyrządem. Mówi, że musi sprawdzić poprawność działania klimatyzacji. Sprawdzał już w innych pomieszczeniach i teraz kolej na moje. Zakłada maskę podobną do takiej, którą noszą lakiernicy, i prosi, żeby na chwilę wyjść z pomieszczenia. Żeby skutecznie dokonać pomiarów systemu chłodzenia, musi rozpylić środek, który może wywołać złe samopoczucie. Zapewnia, że nie zajmie to więcej niż 15 minut. Na tę chwilę wyskoczę akurat do pobliskiej piekarni i kupię dobry chleb na jutro – nie będzie konieczności wczesnego zrywania się na nogi w sobotni poranek. Przed wyjściem blokuję system komputerowy. Nie mogę przecież pozwolić na to, by ktoś „dogrzebał" się do wrażliwych danych, które znajdują się na twardym dysku mojego komputera.

Akt III

Piątek, 15:30

Rozwścieczony szef wpada do mojego pokoju. Rzuca mi na biurko plik kartek. Mówi, że właśnie wydrukował to, co któryś z jego znajomych znalazł w Internecie i podesłał mu pocztą e-mail. Nie mogę uwierzyć własnym oczom! To właśnie ten raport, który był przeze mnie przygotowywany przez ostatni tydzień. Na giełdzie gracze masowo kupują akcje naszej spółki. Ale skąd ktoś wziął ten raport?! Jak go zdobył?! To na pewno przeciek z wydziału, który zajmuje się publikacją!

Nigdy nie przyszłoby mi do głowy, że nowy administrator, który uratował mnie przed kłopotami z komputerem w poniedziałek, i młody człowiek sprawdzający system klimatyzacji to ta sama osoba... A na dodatek pendrive to takie małe urządzenie... Któż mógłby przypuszczać, że te piętnaście minut – przeznaczone na zakupy w piekarni – w zupełności wystarczy na przekopiowanie raportu... Przecież mam tak bardzo skomplikowane hasło do komputera...

Tak oto w przejaskrawiony sposób został przedstawiony atak przestępcy, który niezbędne dla siebie dane pozyskał z wykorzystaniem taktyk socjotechnicznych. W rzeczywistości tego typu działania prowadzone są przy użyciu bardziej wyrafinowanych metod i wymagają od hakera odpowiedniego przygotowania oraz przeprowadzenia dokładnego rozpoznania wnętrza organizacji, z której mają zostać wykradzione informacje. Aby atak mógł zakończyć się sukcesem, przestępca musi zidentyfikować słabe punkty organizacji oraz wyszukać podatności w systemach bezpieczeństwa. W tym celu przed dokonaniem ataku prowadzi on działania mające na celu dogłębne rozpoznanie struktury wewnętrznej firmy, poznanie listy pracowników, zadań przez nich realizowanych, ich znaczenia dla organizacji, numerów telefonów czy adresów e-mail. W obszarze jego zainteresowania znajduje się nawet hobby poszczególnych osób, od których możliwe byłoby uzyskanie ważnych informacji o firmie poprzez dotarcie do nich po godzinach pracy, np. w trakcie zajęć na siłowni, joggingu czy choćby podczas wspólnej gry na polu golfowym. Ważnym elementem jest również analiza fizycznych zabezpieczeń organizacji, sposobu dostępu do jej budynków i poszczególnych pomieszczeń, poznanie procedur dotyczących ruchu osobowo-materiałowego, analiza rozmieszczenia posterunków ochrony fizycznej, obszarów objętych systemem telewizji przemysłowej, a nawet ustalenie listy podmiotów zewnętrznych, realizujących różnego rodzaju usługi na rzecz rozpoznawanej firmy. Osoba, która ma zamiar dostać się na teren zakładu, może posłużyć się fałszywymi dokumentami, sfabrykowanymi przepustkami, wizytówkami. Często jednak informacja będąca celem ataku pozyskiwana jest poprzez elektroniczne kanały dostępu, a odpowiednio zmanipulowani pracownicy organizacji potrafią ją wysłać chociażby przy wykorzystaniu poczty elektronicznej, nierzadko na sfabrykowany adres e-mail przestępcy, który do złudzenia może przypominać adres firmowy.

Profesjonalnie przygotowany atak przeprowadzany jest w taki sposób, że osoba, od której wyłudzono poufne dane, często nawet nie zdaje sobie sprawy z tego, że padła ofiarą przestępstwa.

Jak się ustrzec przed tego typu przestępstwami? Odpowiedź na to pytanie nie jest prosta, a recepty na stuprocentową ochronę nie ma. Można jednak spróbować zminimalizować ryzyko wystąpienia tego typu sytuacji. Już dawno udowodniono, iż najsłabszym ogniwem w każdym systemie bezpieczeństwa są ludzie. Nie pomoże tutaj w związku z tym instalacja dodatkowej kamery, zatrudnienie kolejnego pracownika ochrony czy instalacja kolejnego zabezpieczenia informatycznego. Każdy z tych elementów może stać się następną przeszkodą dla przestępcy, lecz profesjonalista po skutecznie przeprowadzonym rozpoznaniu znajdzie sposób na ominięcie również jej. Konieczne jest zatem wprowadzenie odpowiednich procedur, sformalizowanie wewnętrznego obiegu informacji, wprowadzenie jasnych kryteriów klasyfikacji informacji. Ważnym czynnikiem jest również stałe zwiększanie wiedzy pracowników dotyczącej bezpieczeństwa informacji poprzez szkolenia czy prezentacje. Ale czy te działania skutecznie zabezpieczą przed wypływem poufnych informacji na zewnątrz naszej firmy? To już zależy tylko od każdego z nas...

Krzysztof Białek

Uniwersalny komunikator alarmowy GSM/GPRS GS3055

Przedstawiamy Państwu uniwersalny komunikator alarmowy GSM/GPRS, który może pracować jako podstawowy lub pomocniczy nadajnik alarmowy. Głównym zadaniem urządzenia jest wysyłanie wiadomości tekstowych SMS na zaprogramowane numery telefonów komórkowych, informując o zaistniałych alarmach w systemie. GS3055 ma także możliwość sterowania systemem alarmowym, poprzez wysyłanie odpowiednio zaprogramowanych wiadomości tekstowych na numer telefoniczny karty SIM umieszczonej w urządzeniu. Dzięki wyżej wymienionym funkcjom, nadajnik GS3055 idealnie nadaje się do montażu w domach jednorodzinnych, biurach, jak i mieszkaniach.

GS3055 kompatybilny jest z każdą centralą alarmową obsługującą format Contact ID. Nadajnik łączy dialer centrali alarmowej z siecią GSM i wysyła kody raportujące bezpośrednio do stacji monitorowania wyposażonej w odbiorniki Sur-Gard SYSTEM II/III. Urządzenie GS3055 pracując jako pomocniczy komunikator alarmowy, wysyła wszystkie informacje za pośrednictwem linii naziemnej PSTN, a w przypadku usterki przełącza się automatycznie na sieć GSM, powiadamiając stację monitorowania.
Dla użytkowników, którzy nie posiadają na swoich obiektach linii naziemnej PSTN, nadajnik GS3055 może zostać użyty jako podstawowy komunikator.

Cechy urządzenia

- możliwość wysyłania wiadomości tekstowych SMS informujących o zdarzeniach w systemie na zaprogramowane numery telefonów komórkowych,
- 4 wyjścia OC na płycie,
- 4 wejścia na płycie,
- kompatybilny z każdą centralą alarmową obsługującą format Contact ID,
- raportowanie wszystkich zdarzeń zaistniałych w systemie,
- tania, szybka oraz skuteczna transmisja alarmu poprzez GPRS do odbiornika IP,
- kompatybilny z odbiornikami Sur-Gard SYSTEM II/III.

Wyłączny dystrybutor w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 022 546 05 46, fax 022 546 05 01
www.aat.pl

Profesjonalizm w zarządzaniu bezpieczeństwem firmy

Autor, odnosząc się do złożonej problematyki wynikającej z konieczności zapewnienia bezpiecznego funkcjonowania firmy oraz pisząc o konieczności edukowania kadry zarządzającej w tym zakresie, wskazuje grupy procesów mających bezpośredni wpływ na bezpieczeństwo firmy i jej sukcesy. Podpowiada, jakie działania menedżerskie należy podjąć oraz czemu w codziennej praktyce wypada szczególnie się przyjrzeć, aby – w wyniku zbiegu niekorzystnych zdarzeń i własnej niefrasobliwości – nie zostać zaskoczonym niespodziewanymi stratami (finansowymi, informacyjnymi i rynkowymi)

Tytułem wstępu …

Bezpieczeństwo jest przez człowieka rozumiane intuicyjnie jako brak widocznych zagrożeń, ale próba sformułowania jego jednej i zarazem jednoznacznej definicji napotyka na szereg trudności – merytorycznych, językowych i kulturowych. Działania człowieka pod tym względem mają podstawy naturalne, ale są modyfikowane nabytymi nawykami i procesami kulturowymi w jego bezpośrednim otoczeniu (przysłowiowa już „moralność Kalego").

„(...) Instynkt poszukiwania bezpieczeństwa sięga początków świata ożywionego i tworzy istotny element ciągłości w jego ewolucji. Dotyczy to zarówno jednostek jak i zbiorowości – od mrowisk po narody i państwa (...)" (A. Töfller)

Wiele dyskusyjnych nieporozumień w ocenie bezpieczeństwa człowieka, firmy, państwa jest skutkiem braku świadomości i złego rozumowania. W ferworze przekonywania i udowadniania swoich racji rozmówcom zapomina się bowiem o istotnym fakcie: bezpieczeństwo nie jest stanem – jest ciągle zmieniającym się procesem, którego wewnętrzne i zewnętrzne uwarunkowania są, w różnym (czasami niewielkim) stopniu, zależne od osoby, organizacji, społeczności, której bezpośrednio dotyczą.

Kilka słów o teorii samego zjawiska

Obszar bezpieczeństwa człowieka stał się w ostatnich latach XX wieku domeną działalności naukowej – securitologii, uwzględniającej wieloaspektowość postrzegania i „odczytywania" bezpieczeństwa jako obiektu badań.

Pierwsze publikacje podejmujące próbę wyodrębnienia securitologii jako dyscypliny naukowej pochodzą z 1989 r., co można wyjaśnić nowymi potrzebami i oczekiwaniami, a także warunkami kształtującymi się po rewolucyjnej zmianie ustrojów społeczno-politycznych w Europie.

Cechą charakterystyczną dla tych właśnie publikacji jest opisanie i uwzględnienie wielorakich czynników: obiektywnych i subiektywnych, socjopsychologicznych i kulturowych, politycznych i prawnych, przyrodniczych i technicznych, makro- i mikroekonomicznych, które nie tylko warunkują zagrożenia, ale także pozostają z nimi we wzajemnych nierozerwalnych związkach.

Nauka o bezpieczeństwie (securitologia) jest w chwili obecnej widziana dwojako i jest traktowana jako:

- dyscyplina naukowa w grupie 64 (nauki interdyscyplinarne), tzn. poświęcona badaniom naukowym dotyczącym bezpieczeństwa;
- poddziedzina nauki, ulokowana w ramach systematyzacji odpowiednio w grupie 3 (nauki ekonomiczne) i w dziedzinie 2 (nauki o zarządzaniu, tzn. badanie procesów zarządzania bezpieczeństwem).

Powyższe wynika z szeregu praktycznych osiągnięć zrealizowanych w badaniu teorii i praktyki bezpieczeństwa człowieka w ramach securitologii w okresie ostatnich lat – przy liczącym się współudziale polskiego środowiska naukowego oraz prac popularyzatorskich Stowarzyszenia EAS (*European Association for Security*).

Zapoznanie się z bieżącym dorobkiem publicystycznym i normatywnym, dotyczącym bezpieczeństwa w rozumieniu potrzeb człowieka i firmy, jest dla personelu kierowniczego potrzebą chwili – ciągłe zmiany w stosunkach gospodarczych, asymetryczny układ zagrożeń wojennych oraz narastające zagrożenie ze strony terroryzmu są istotnymi czynnikami wpływającymi na pozycję danej firmy na rynku. Dla firm ponadnarodowych (korporacje, holdingi) problematyka ta jest czymś oczywistym, ale warto zwrócić uwagę na zmiany w zakresie bezpieczeństwa firm w rozumieniu ich funkcjonowania na rynkach lokalnych – wymaga to chwili roztropnego zastanowienia…

Stowarzyszenie EAS jest towarzystwem naukowym, które prowadzi badania i popularyzuje nauki o bezpieczeństwie człowieka. EAS powstało na konferencji krakowskiej 12 maja 2000 r. i posiada osobowość prawną. Celem Stowarzyszenia jest edukacja dla bezpieczeństwa ludzi i firm we wspólnej Europie. Adres, statut, lista członków i inne dokumenty są dostępne na stronie www.eas.krakow.pl.

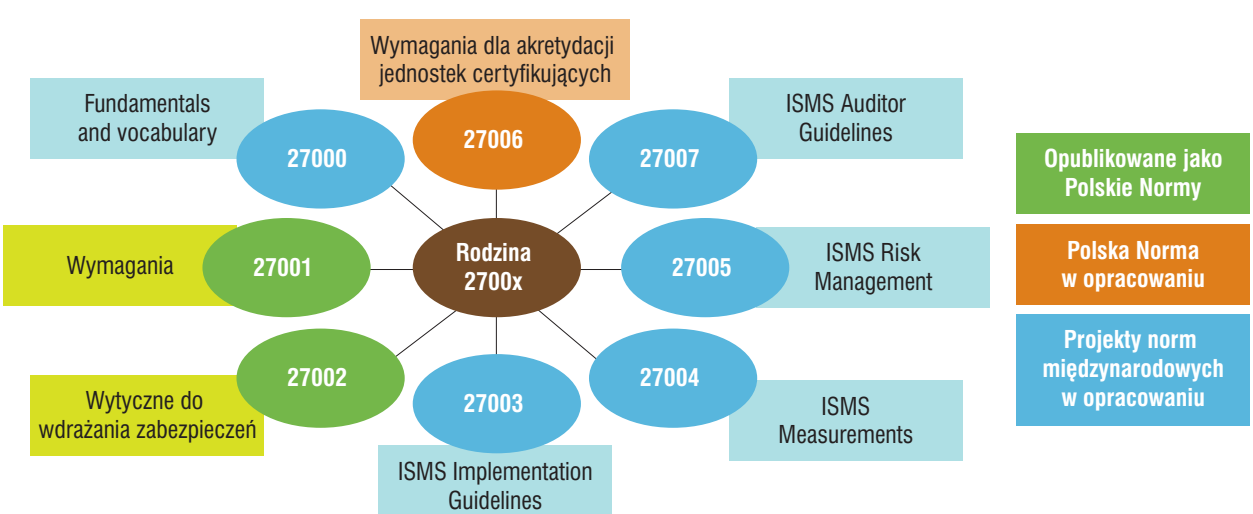
Stowarzyszenie wydaje publikacje książkowe oraz – na bieżąco – zeszyty naukowe *Securitologia/Securitology/Секьюритология,* dotyczące nauk o bezpieczeństwie oraz zagadnień z zakresu edukacji dla bezpieczeństwa.

Warto wiedzieć, że na podstawie programowej wypracowanej przez Stowarzyszenie prowadzone są studia wyższe w specjalnościach: zarządzanie bezpieczeństwem, bezpieczeństwo europejskie, administracja bezpieczeństwem, a także studia podyplomowe: zarządzanie bezpieczeństwem, edukacja dla bezpieczeństwa. Funkcjonuje także Międzynarodowy Ośrodek Szkoleń Specjalnych.

Równolegle (ze względu na czas zdarzeń) rozwijana jest związana z bezpieczeństwem informacji i problematyką zarządzania nim międzynarodowa działalność normatywna połączonego komitetu organizacji ISO i IEC (data 15 grudnia 2000 roku oznacza przyjęcie przez JTC1/SC27 ISO/IEC pierwszej międzynarodowej normy zarządzania bezpieczeństwem ISO 17799 – powstałej na bazie normy brytyjskiej BS 7799).

Aktualnie istnieje (ciągle rozbudowywana) rodzina norm ISO 27000 w całości poświęcona problemom bezpieczeństwa informacji i zarządzania, a jej powiązania ukazuje poniższy rysunek (norma ISO/IEC 27005 została opublikowana dnia 5 lipca 2008 roku w Genewie).

Kwestia unormowania sposobów zarządzania bezpieczeństwem, postępowania z ryzykiem oraz zabezpieczenia informacji w procesach zarządczych i poza nimi jest od roku 2000 priorytetem działań komitetu SC27 i jego grup roboczych (WG 1-5) w zakresie zaspokojenia potrzeb i oczekiwań społecznych w tym względzie, przy zachowaniu warunków standaryzacji bezpieczeństwa jako takiego.



Rys. 1. Rodzina norm zarządzania bezpieczeństwem

1. Zarządzanie bezpieczeństwem – profesja czy profesjonalizm zawodowy

Pojęcie profesji jako wyspecjalizowanego zawodu ma wielowiekowy rodowód (cechy rzemieślnicze w średniowieczu) i w odczuciu społecznym wiąże się z doskonałością wykonywanej pracy. Szeroko rozpowszechniony jest pogląd, że profesje powstają, by zaspokajać określone potrzeby zbiorowości, gwarantować wysoki poziom usług. Stąd termin *profesjonalizm*, który oznacza wysoki standard wykonania danej czynności. Określenia pochodne odnoszone są do różnych dziedzin współczesnego życia (np. profesjonalizacja armii – jako określenie jej uzawodowienia; reklamowana profesjonalność usług; intratna profesja – jako określenie wysoko opłacanego zawodu itp.).

Czy zarządzanie bezpieczeństwem można uznać za wyodrębniony zawód – profesję? Odpowiedź na tak postawione pytanie jest tylko pozornie prosta – można i trzeba, ale pod warunkiem uzupełnienia/dookreślenia poprzez przypisanie zakresu/obszaru tego zarządzania, bowiem wypada jednoznacznie określić, jakie/czyje bezpieczeństwo tym zarządzaniem chcemy zapewnić. Truizmem jest tutaj przypominanie, że jeśli „(…) ktoś mówi, że robi wszystko – to sam nie robi nic" (J. Piłsudski, *Pisma wybrane*, Warszawa 1932).

W firmie mamy szereg obszarów, o których bezpieczeństwo powinniśmy dbać w sposób szczególny. Są to miejsca, w których gromadzimy:

- tajemnice przedsiębiorstwa (w tym informacje biznesowe własne i powierzone);
- dane osobowe pracowników, klientów i kontrahentów;
- mienie o znacznej wartości (własne i powierzone);
- materiały archiwalne o wymaganym okresie udostępniania (szczególnie z zakresu finansowo-księgowego, dokumentacja zatrudnienia itp.).

Nie wolno zapominać przy tym o ogólnej ochronie fizycznej i technicznej obiektu firmy oraz o jego bezpieczeństwie środowiskowym (bhp, ochrona ppoż., ewakuacja itd.).

Na poziomie „odpowiedzialnego za wszystko" ustawowego kierownika jednostki organizacyjnej (w praktyce stojącego na czele firmy prezesa – dyrektora generalnego) zarządzanie bezpieczeństwem ma charakter decyzyjny i skupione jest z zasady na następujących kierunkach/obszarach:

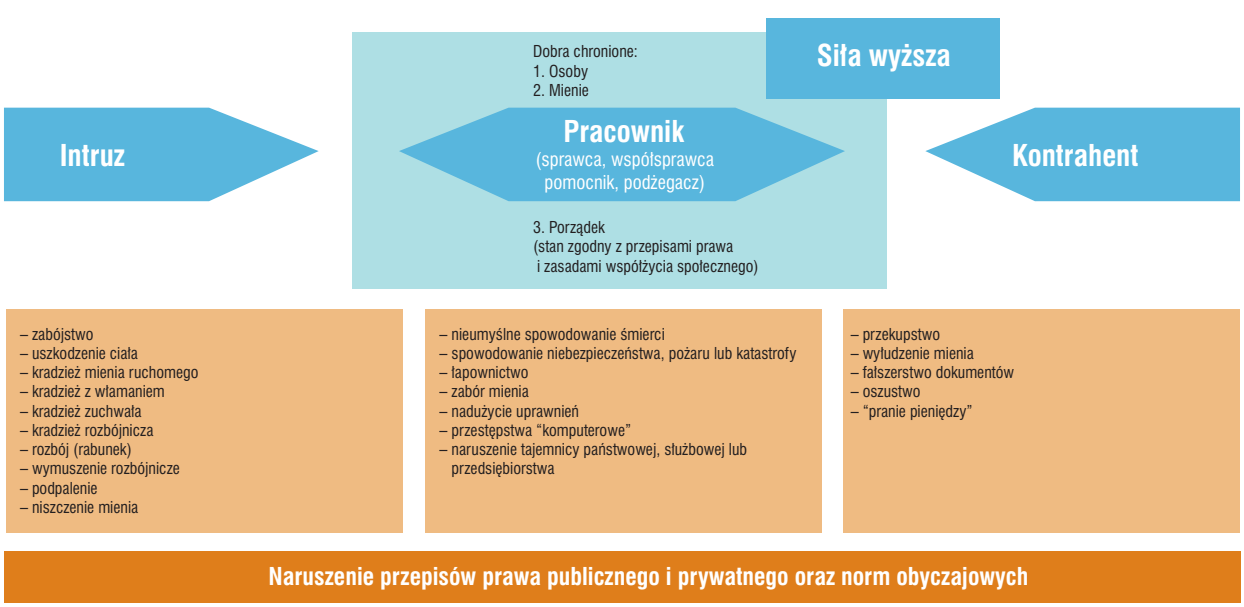
- zarządzanie bezpieczeństwem organizacyjnym (głównie personalnym);
- zarządzanie bezpieczeństwem fizycznym (ochrona osób i mienia);
- zarządzanie bezpieczeństwem informacyjnym (informacje, dane, zasoby I&CT);
- zarządzanie bezpieczeństwem kryzysowym – zachowaniem ciągłości działania.

Rozbieżność wymagań szczegółowych w każdym z tych obszarów (osadzenie prawne, realia funkcjonowania, różnorodność zagrożeń, charakter ponoszonego ryzyka, skuteczność działania) jest przyczynkiem do wyodrębnienia specjalizacji zarządczej (niezbędne jest opanowanie szczegółów prawnych i praktyka ich stosowania), co stawia pod znakiem zapytania możliwości i zakres niezbędnych umiejętności zawodowych (profesję) pojedynczej osoby mającej je wszystkie opanować przy jednoczesnej zdolności i gotowości do poprawnego kierowania firmą w zakresie biznesowym i operacyjnym.

Czy można rozstrzygnąć tę sprzeczność? Warto ten problem widzieć jako „profesjonalizm władzy", czyli poprawność działania ogólno-zarządczego, wyrażającego się w powołaniu na poziomie najwyższego kierownictwa osoby (np. pełnomocnika zarządu) na tyle zorientowanej w kwestiach bezpieczeństwa firmy, aby móc jej powierzyć odpowiedzialność za te właśnie obszary oraz udostępnić związane z nią uprawnienia decyzyjne (organizacyjne i finansowe). Od takiego funkcjonariusza można wówczas wymagać profesjonalnego działania (po zapewnieniu mu odpowiedniego certyfikowanego przeszkolenia) i zapewnienia całości bezpieczeństwa na takim poziomie, jaki jest wymagany i niezbędny w danej firmie.

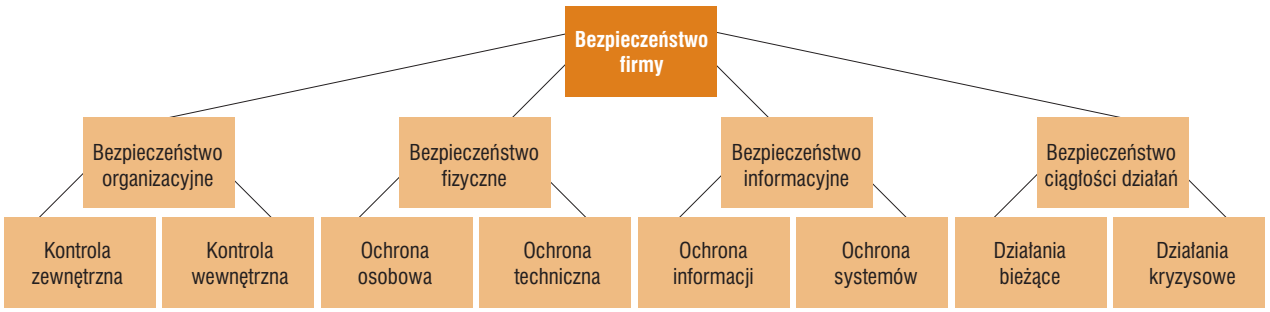
2. Zagrożenia bezpieczeństwa we współczesnej firmie

Doświadczenia zebrane w okresie transformacji ustrojowej Polski w znaczącym stopniu wpłynęły nie tylko na wprowadzane definicje bezpieczeństwa społecznego, ale przede wszystkim na jego odczucie w codzienności biznesowej firmy. Aktywność rynkowa nie tylko wprowadziła na polski rynek własnych przedsiębiorców, ale znacząco go zmieniła poprzez udział konsorcjów i agend międzynarodowych, ujawniając nie zawsze



Rys. 2. Źródła zagrożeń dla osób, mienia i porządku

Źródło: Fehler Wł. (red.), Bezpieczeństwo w biznesie, Messenger Service Stolica S.A., Warszawa 2005, s. 117



Rys. 3. Obszary zarządzania bezpieczeństwem w firmie

korzystne zjawiska (przysłowiowe już widmowe „firmy krzaki", *leasing fraud*, liczne przekręty towarowe i finansowe związane z akcyzą, zwrotem VAT itp.). Zagrożeniem dla firmy stały się nie tylko warunki zewnętrzne (niestabilność rynku, nieuczciwi kontrahenci), ale i wewnętrzne (zaniedbania ochrony danych, kradzież tajemnic przedsiębiorstwa, nieuczciwy personel własny i zapewniany przez outsourcing), nie zawsze będące ewidentnymi przestępstwami, ale poprzez swoją częstość przynoszące wymierne straty i szkody w codziennym funkcjonowaniu firmy.

Działania zarządcze na rynku (planowane w ujęciu biznesowym) okazały się źródłem łatwiejszych do zlokalizowania i wyeliminowania incydentów i zagrożeń niż operacyjne funkcjonowanie samej firmy – szczególnie jeśli, w trosce o redukcję kosztów, szereg wewnętrznych czynności usługowych powierzono firmom zewnętrznym, których priorytety znacząco odbiegają od oczekiwań zlecającego. Jeżeli dodamy do tego ofensywę wywiadowni gospodarczych oraz firm zajmujących się wyszukiwaniem i rekrutacją pracowników („łowców głów" – ang. *head hunters*), to wówczas oczywiste staje się stwierdzenie, że „współcześnie 80% zagrożeń firmy pochodzi z jej wnętrza" (dane wg FBI USA; 04.2005).

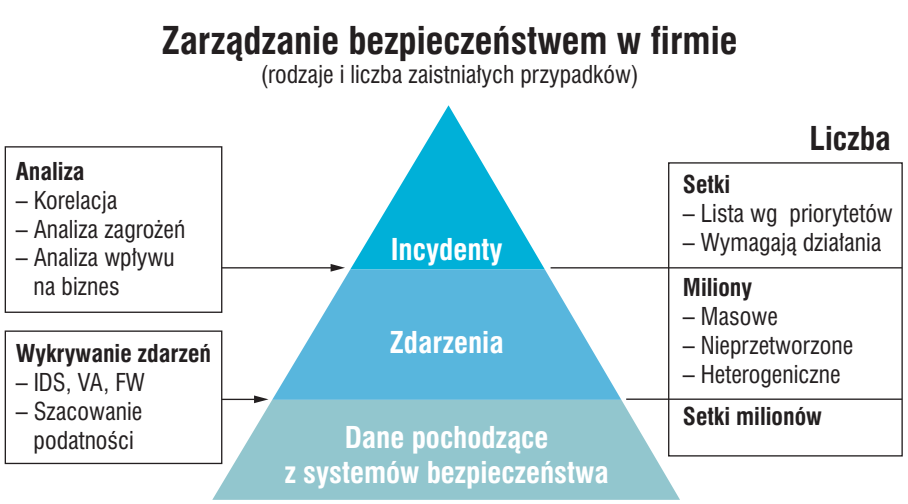
Przyjmując (za gen. Zbigniewem T. Nowickim), że zakres dóbr chronionych obejmuje osoby, mienie oraz porządek, i nie zapominając o skutkach zaistnienia siły wyższej (katastrofy naturalnej lub wywołanej przez człowieka, stanów kryzysowych oraz nadzwyczajnych), musimy szczególnie wnikliwie przyjrzeć się działaniom własnych pracowników.

Pojawia się zatem socjologiczna sprzeczność: musimy zaufać pracownikom, powierzając im istotne dane i tajemnice firmy, a zarazem liczyć się z koniecznością kontroli ich pracy. Problem ten musi być rozwiązywany wielopłaszczyznowo: organizacyjnie, personalnie i informacyjnie, przy spełnieniu wymagań ochrony bezpośredniej (fizycznej i technicznej), a szczególnie w odniesieniu do zespołów ludzkich zapewniających ciągłość działania firmy.

3. Obszary zarządzania bezpieczeństwem w firmie

Powierzenie zarządzania bezpieczeństwem firmy wiąże się bezpośrednio z odrębnością uregulowań prawnych (rozporządzeń UE i dokumentó w ustawowych RP) i z tego względu (odrębności strukturalne oraz penalne) skupione jest na głównych kierunkach zarządzania bezpieczeństwem w firmie, tzn. na:

1. **bezpieczeństwie organizacyjnym, obejmującym kontrolę stanu:**
   - zewnętrznego (dotyczy to szczególnie bezpieczeństwa biznesowego i administracyjno-prawnego);
   - wewnętrznego (dotyczy to szczególnie audytów i przeciwdziałania penetracji);
2. **bezpieczeństwie fizycznym, obejmującym kontrolę stanu:**
   - ochrony osób (dotyczy to szczególnie personelu własnego, ale także osób zewnętrznych: klientów, stażystów, outsourcingu usług);
   - ochrony technicznej (dotyczy to szczególnie zagrożeń danych i mienia oraz rozwiązań ewakuacyjno-ratunkowych);
3. **bezpieczeństwie informacyjnym, obejmującym wszystkie działania ochronne prowadzone na rzecz:**
   - zapewnienia bezpieczeństwa (poufności, integralności i dostępności) informacji własnych i powierzonych – niezależnie od charakteru zasobu;
   - zapewnienia ochrony systemów przetwarzania informacji (dane doraźne, zasoby archiwizowane, systemy I&CT);
4. **bezpieczeństwie kryzysowym, związanym z zachowaniem ciągłości działania firmy w różnych warunkach, obejmującym:**
   - bieżące przeciwdziałanie incydentom i zagrożeniom (niedopuszczenie do materializacji wynikających z nich ryzyk);
   - działania bieżące w warunkach kryzysowych (scenariusze kryzysowe i plany działania firmy w sytuacjach nadzwyczajnych).



Rys. 4. Schemat krotności zdarzeń niebezpiecznych

Układ tych zależności można przedstawić graficznie jako „drzewo celów" i opracowywać pod względem zarządczym (cele, decyzje, skutki, zależności) z wykorzystaniem metody PATTERN.

Pojawiające się w praktyce codziennej działalności firmy różnorodne zagrożenia można przewidywać, ale, aby im zapobiegać, należy zwracać szczególną uwagę na ich wcześniejsze symptomy i analizować zaobserwowane incydenty z zakresu naruszeń bezpieczeństwa. Zasadność takiego działania stanie się oczywista, jeżeli dokonamy weryfikacji zgłoszeń wszystkich przypadków związanych z bezpieczeństwem oraz uzupełnimy to działanie o weryfikację raportów o próbie wejścia/włamania pochodzących z automatycznych zabezpieczeń (fizycznych, technicznych, informatycznych).

Istotny jest tutaj czynnik czasu – analiza zagrożeń wynikających z incydentów jest możliwa na drodze działań bezpośrednich człowieka nawet w bardzo dużej firmie, o ile została przygotowana prawidłowa lista priorytetów i określono zakres i sposób działania wobec standaryzowanych objawów incydentów. W każdym innym przypadku powiększa się jedynie prawdopodobieństwo przepuszczenia bez oddziaływania sygnałów świadczących o zagrożeniach, aż do momentu wystąpienia bezpośrednich zdarzeń i przypadków materializacji ryzyk. Profesjonalne przygotowanie w małej albo średniej firmie jednej osoby odpowiedzialnej za całość bezpieczeństwa pozwala na prawidłowe agregowanie wszystkich tego typu zjawisk i skuteczne przeciwdziałanie ich negatywnym objawom. W firmach średnich, o dużym obszarze zdarzeń, może być konieczne dodatkowe wyspecjalizowanie zawodowe osób zajmujących się pojedynczymi obszarami bezpieczeństwa, a czasami wskazane jest powołanie zespołów ludzi dla danego obszaru (np. wymóg ustawowy Pionu Ochrony Informacji Niejawnych).

W warunkach rozległych organizacji krajowych i międzynarodowych działają wyodrębnione komórki organizacyjne (działy, biura i wydziały bezpieczeństwa), co stwarza dodatkowe problemy w zakresie zrozumiałej i wspólnej wymiany informacji o niebezpieczeństwie.

4. Profesjonalizm w zarządzaniu bezpieczeństwem firmy

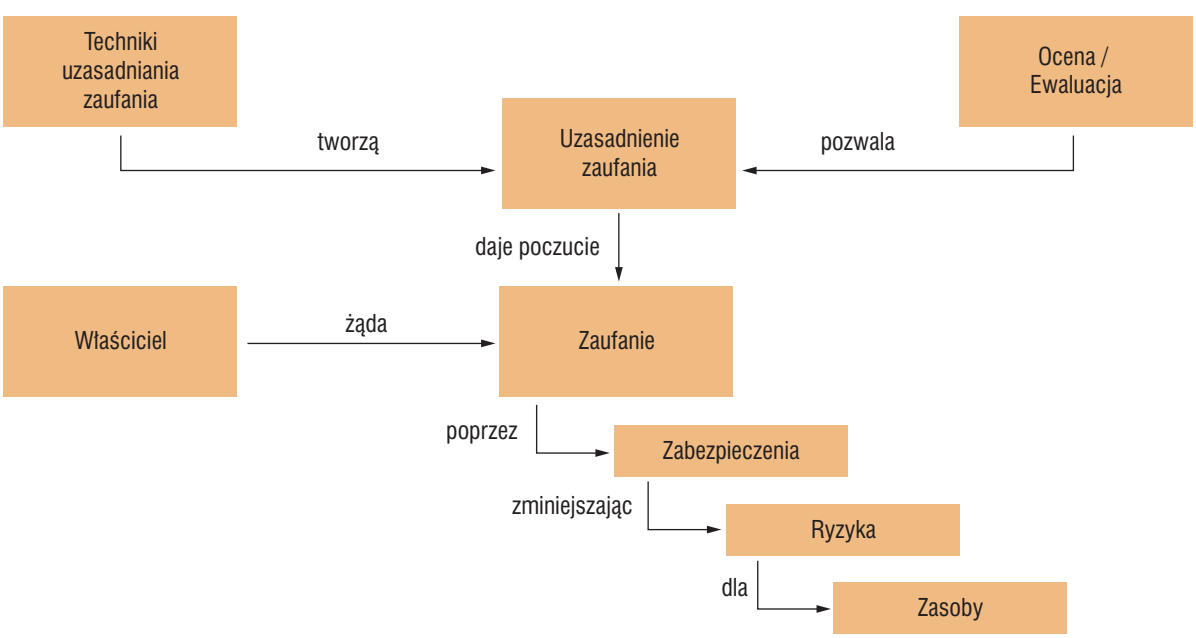
Profesjonalizacja czynności związanych z bezpieczeństwem wiąże się w sposób nierozerwalny z zaufaniem właściciela do wszystkich podejmowanych i realizowanych działań oraz osób je wykonujących. Rozległość polskiego prawa i przyjęte zobowiązania unijne powodują, że, aby być profesjonalistą w zarządzaniu bezpieczeństwem, trzeba posiadać dobrą znajomość zdarzeń i dogłębną praktykę, a zarazem umieć uzyskać i uzasadnić zaufanie do prowadzonej działalności.

W chwili obecnej nie można bezkarnie powierzać bezpieczeństwa firmy osobom nieprzygotowanym, ale zarówno właścicielom, jak i zarządcom przydałaby się chwila zastanowienia nad własnym rozumieniem tych problemów, o czym warto przypomnieć.

DR INŻ. MAREK BLIM

Bibliografia:

1. Fehler Wł. (red.), *Bezpieczeństwo w biznesie*, Messenger Service Stolica S.A., Warszawa 2005.
2. Jemielniak D., *Kultura – zawody i profesje*, [w:] *Prace i materiały Instytutu Studiów Międzynarodowych SGH*, nr 32, Warszawa 2005, s. 7–22.
3. Konieczny J., *Wprowadzenie do bezpieczeństwa biznesu*, Konsalnet, Warszawa 2004.
4. Meister D. H., *Prawdziwy profesjonalizm*, Studio Emka, Warszawa 2001.
5. Materiały VI kursu przygotowawczego do rzeczoznawstwa STZOiMoZB, opracowanie TECHOM – POLALARM, Warszawa 2006–2007.
6. Sikorski Cz., *Profesjonalizm. Filozofia zarządzania nowoczesnym przedsiębiorstwem*, PWN, Warszawa 1995.
7. Sikorski Cz., *Drogi do sukcesu. Profesjonalizm kontra populistyczna kultura organizacyjna*, Difin, Warszawa 2007.
8. Zagórski Z., *Socjologiczne portrety grup społecznych*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2002.



Rys. 5. Zależności bezpieczeństwa informacji w firmie
Źródło: Biała A., materiały XVI Jubileuszowej Górskiej Szkoły PTI, Szczyrk 2004

Zarządzanie ryzykiem
w działalności gospodarczej (część 3)

Zanim przybliżymy, zgodnie z zapowiedzią z części 2 artykułu, tematykę szacowania ryzyka, zostanie bardziej szczegółowo omówiony przedstawiony w poprzednim artykule model zarządzania ryzykiem RMTP

Model RMTP

W omawianym modelu wstępem do procesu zarządzania ryzykiem jest ustalenie kontekstu czy obszaru albo, jak przedstawiają to firmy informatyczne, wymiaru zarządzania ryzykiem. Ta część zdecydowanie należy do najwyższego kierownictwa firmy, które w porozumieniu z menedżerem ryzyka lub z zespołem zarządzania ryzykiem podejmuje decyzję o wdrożeniu tego procesu w firmie. Następnie najwyższe kierownictwo zobowiązane jest do ustalenia kryteriów (inaczej można je nazwać „warunkami brzegowymi") zarządzania ryzykiem. Co to oznacza?

W procedurze szacowania ryzyka, stanowiącej najważniejszy element procesu zarządzania ryzykiem, porównujemy otrzymane wyniki identyfikacji i analizy ryzyka z założonymi kryteriami i podejmujemy akcję zarządzania ryzykiem lub akceptujemy ryzyko, zgodnie z przyjętymi dla danego kontekstu kryteriami akceptacji. Często akceptację uważa się za formę podjęcia ryzyka, ale dla przejrzystości i zrozumienia tematu zostało to wyszczególnione w odrębnym bloku ww. modelu.

Podejmowanie ryzyka to wykonywanie działań zmniejszających negatywne skutki wystąpienia straty, czyli ryzyka negatywnego, lub pomagających wykorzystać możliwości wystąpienia szansy, tzw. ryzyka pozytywnego (wg angielskiego tłumaczenia). Pozostańmy jednak w przyszłości przy nomenklaturze polskiej, czyli mówmy o szansie. W trakcie postępowania z ryzykiem mogą pojawić się nowe okoliczności, które spowodują, że powinniśmy zaplanować wystąpienie nowych ryzyk. Teoretycznie można uważać, że taki moment stanowi element szacowania ryzyka. Tak nie jest, ponieważ planowanie nowych ryzyk na etapie postępowania z ryzykiem wymaga wskazania ich menedżerowi ryzyka lub zespołowi zarządzania ryzykiem w celu uwzględnienia ich podczas wykonywania kolejnej procedury szacowania ryzyka.

Po wykonaniu procedur dotyczących postępowania z ryzykiem należy przeprowadzić monitoring ryzyka na podstawie wiarygodnych analiz i pomiarów, a następnie albo uznać ryzyko za zmodyfikowane i przekazać informację najwyższemu kierownictwu w celu akceptacji ryzyka szczątkowego lub podjęcia decyzji w sprawie konieczności zmiany kryteriów, albo na nowo przeszacować ryzyko.

W przypadku ponownego przeszacowania ryzyka i podjęcia kolejnych kroków postępowania z ryzykiem wykonuje się następnie czynności opisane w poprzednim akapicie.

W naszej ocenie na każdym etapie procesu zarządzania ryzykiem konieczna jest komunikacja pomiędzy członkami zespołu zarządzania ryzykiem, najwyższym kierownictwem, właścicielami ryzyk i wszystkimi osobami uczestniczącymi w poszczególnych fazach zarządzania ryzykiem.

Przedstawiony model pokazuje proces zarządzania ryzykami mniejszej wagi (strzałki koloru niebieskiego), które nie wymagają bieżącego informowania najwyższego kierownictwa i wiążą się ze sprawami operacyjnymi na poziomie kierowników komórek organizacyjnych, oraz proces zarządzania ryzykami, w których powinno uczestniczyć najwyższe kierownictwo (strzałki koloru pomarańczowego) i które mają wpływ na realizację strategii firmy w odniesieniu do realizacji jej celów biznesowych. Nie zapominajmy również o tym, że nawet najmniej znaczące ryzyko może się w warunkach sprzyjających (podatność) przekształcić w ryzyko krytyczne, uniemożliwiające realizację celu biznesowego firmy, i odwrotnie, co również uwzględniono w przedstawionym modelu. Nasze artykuły mówią o firmie i jej celach biznesowych, ale potraktujmy to jako przykład. Modele zarządzania ryzykiem można stosować tak samo w przypadku organizacji i osiągania przez nie celów statutowych, jak i urzędów administracji publicznej i osiągania przez nie celów wynikających z przepisów prawa.

Szacowanie ryzyka

W niniejszej części artykułu dotyczącego zarządzania ryzykiem w działalności gospodarczej postaramy się przedstawić bardzo istotny, w istocie najważniejszy element zarządzania ryzykiem, którym jest szacowanie ryzyka. W poprzedniej części artykułu został zaprezentowany schemat albo raczej model zarządzania ryzykiem, w którym znajduje się element **„szacowania ryzyka wg metodologii odpowiadającej kontekstowi ryzyka".**

Aby móc zarządzać ryzykiem, w pierwszej kolejności należy je oszacować. Przytoczymy Państwu kilka definicji związanych z szacowaniem ryzyka, zaczerpniętych z międzynarodowego przewodnika zawierającego nomenklaturę

z zakresu szeroko pojętego zarządzania ryzykiem ISO/IEC Guide 73 „Risk management – Vocabulary".

Szacowanie ryzyka *– całościowy proces identyfikacji, analizy i oceny ryzyka*[1]

Identyfikacja ryzyka *– proces szukania, rozpoznania i opisania ryzyka*[2]

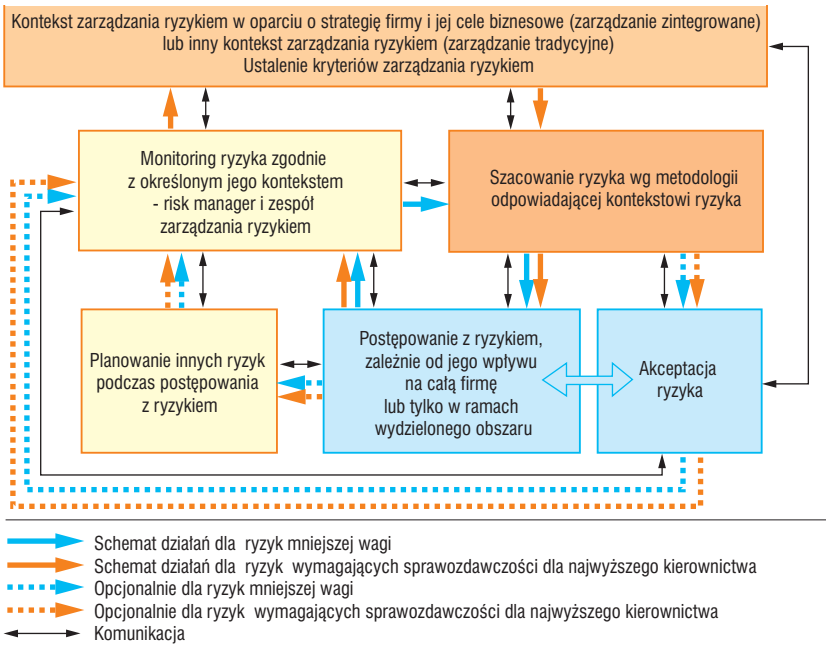
Analiza ryzyka *– systematyczny proces rozumienia natury ryzyka i wnioskowania odnośnie jego poziomu*[3]

Ocena ryzyka *– proces porównania rezultatów analizy ryzyka w stosunku do przyjętych kryteriów ryzyka w celu określenia poziomów ryzyka i przyjęcia akceptowalnych lub nieakceptowanych poziomów ryzyka*[4]

Krótko komentując powyższe definicje, możemy sformułować następujące stwierdzenia:

– proces identyfikacji ryzyka dotyczy identyfikacji źródeł ryzyka, niepożądanych zdarzeń, ich przyczyn lub zaistnienia niepożądanych okoliczności oraz ich potencjalnych konsekwencji,

1) ISO/IEC Guide 73 „Risk management - Vocabulary"
2) ISO/IEC Guide 73 „Risk management - Vocabulary"
3) ISO/IEC Guide 73 „Risk management - Vocabulary"
4) ISO/IEC Guide 73 „Risk management - Vocabulary"



Rys. 1 . Model RMTP © Anna Słodczyk, Piotr Mąkosa

– proces analizy ryzyka dostarcza podstaw do oceny ryzyka i decyzji związanych z późniejszym postępowaniem z ryzykiem,

– proces oceny ryzyka pomaga w podejmowaniu decyzji związanych z postępowaniem z ryzykiem.

W następnej części artykułu przedstawimy Państwu graficzną interpretację procesu szacowania ryzyka według dwóch jakże odległych od siebie modeli zarządzania ryzykiem, to jest normy ISO/IEC 27005[5] oraz AS/NZS 4360[6].

Anna Słodczyk, Piotr Mąkosa
Risk Management Team Poland

5) ISO/IEC 27005
6) AS/NZS 4360:2004

LOKALIZACJA OCHRONA MONITORING

Monitoring
Osób

Monitoring
Firm

Monitoring
Pojazdów

Monitoring
Maszyn

Centrum Monitorowania Alarmów Sp. z o.o.

adresy i telefony biur na
WWW.CMA.COM.PL

Automonitoring Mobilemonitoring Multimonitoring

Zagrożenia bezpieczeństwa informacji w przedsiębiorstwie

część 1 – Istota bezpieczeństwa informacji i klasyfikacja zagrożeń

Współczesne przedsiębiorstwa, zmuszone do prowadzenia działalności w warunkach niepewności i chaosu, poddają modyfikacjom swoje podejście do bezpieczeństwa. W obliczu trudności związanych z niepewnością i chaosem przedsiębiorstwa stoją przed koniecznością brania pod uwagę zarówno zdarzeń lokalnych, jak i globalnych, wpływających na ich działalność

Potrzeba poczucia bezpieczeństwa stanowi jedną z zasadniczych potrzeb człowieka, jest wartością pierwotną i podstawą. Stąd też kategoria bezpieczeństwa agreguje wszystkie składowe najważniejszej dla człowieka wartości. W związku z tym, zaliczając bezpieczeństwo do dóbr podstawowych, należy podkreślić, iż powinno ono stanowić przedmiot szczególnej uwagi w zarządzaniu organizacją gospodarczą niezależnie od form zorganizowania, szczebla hierarchicznego i stopnia rozwoju.

1. Istota bezpieczeństwa informacji

W odniesieniu do postrzegania i poszukiwania poczucia bezpieczeństwa warto wziąć pod uwagę model zaprezentowany przez D. Frei'a, który uwzględnia cztery elementy[1]:

- stan braku bezpieczeństwa – w którym występuje rzeczywiste i istotne zagrożenie zewnętrzne, którego postrzeganie jest adekwatne,
- stan obsesji – w którym niewielkie zagrożenie postrzega się jako duże,
- stan fałszywego bezpieczeństwa – w którym istotne zagrożenie postrzegane jest jako niewielkie,
- stan bezpieczeństwa – w którym zagrożenie zewnętrzne jest niewielkie, a jego postrzeganie prawidłowe.

1) Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 9.

Literatura przedmiotu szeroko omawia pojęcie i typologie bezpieczeństwa z różnych perspektyw. Dokonując ich przeglądu, można zauważyć, iż po pierwsze: charakteryzuje je duży poziom ogólności i odmienność spojrzenia na problem bezpieczeństwa z racji reprezentowania przez autorów różnych dyscyplin naukowych, takich jak lingwistyka, politologia, psychologia, wojskowość i zarządzanie. Po drugie: podstawowym zadaniem przedsiębiorstw jest tworzenie i doskonalenie systemów bezpieczeństwa, przy czym stwarza się poczucie bezpieczeństwa dla pracowników przedsiębiorstw i ich otoczenia. Najszersze rozumienie bezpieczeństwa wyraża się w stwierdzeniu, iż „pewien podmiot jest bezpieczny, jeśli jest zdolny do osiągania swoich celów”[2]. Wydaje się jednak, iż dla potrzeb niniejszego opracowania odpowiednia jest definicja bezpieczeństwa W. Šmid'a, zgodnie z którą bezpieczeństwo to sytuacja odznaczająca się brakiem ryzyka np. w inwestowaniu, planach strategicznych, zasobach materialnych i ludzkich[3].

Bezpieczeństwo informacji to nic innego, jak „obrona informacyjna, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych”[4].

Na każdym poziomie zarządzania bezpieczeństwem informacji zasadniczym celem jest niedopuszczenie do jej ujawnienia. Należy podkreślić, że zbyt szerokie rozumienie bezpieczeństwa może utrudniać przepływ informacji w państwie, przedsiębiorstwie itp. – informacji, które są niezbędne do ich sprawnego i skutecznego funkcjonowania.

Na tym tle jawi się istotna kwestia związana z zagadnieniem bezpieczeństwa informacyjnego, które dotyczy ochrony informacji stanowiących tajemnicę państwową, względnie służbową. Bezpieczeństwo informacyjne w szerokim ujęciu rozumiane jest jako stan wolny od zagrożeń, które z kolei rozumiane są głównie jako:

- przekazywanie informacji nieuprawnionym podmiotom,
- szpiegostwo,
- działalność dywersyjna lub sabotażowa[5].

Bezpieczeństwem informacyjnym jest również każde działanie, system bądź metoda, które zabezpieczają zasoby informacyjne gromadzone, przetwarzane, przekazywane oraz przechowywane w pamięci komputerów i sieciach teleinformatycznych[6]. Dlatego też bezpieczeństwo informacyjne należy rozumieć jako wypadkową bezpieczeństwa fizycznego, prawnego, osobowo-organizacyjnego oraz teleinformatycznego organizacji gospodarczej[7].

Bezpieczeństwo jest procesem ciągłym, w ramach którego przedsiębiorstwa starają się udoskonalać mechanizmy zapewniające im poczucie bezpieczeństwa. Odzwierciedlenie rozumienia i traktowania bezpieczeństwa jako kluczowego obszaru zainteresowań przedsiębiorstw znajdujemy w ich działaniach podejmowanych w obliczu zagrożenia. Działania te są zadaniami trudnymi i kosztownymi, co w wielu przypadkach może stanowić przyczynę ich zaniechania.

Rys. 1. Składowe bezpieczeństwa informacji
Źródło: Łuczak J. (red.), Zarządzanie bezpieczeństwem informacji, Oficyna Współczesna, Poznań 2004, s. 80.

2. Klasyfikacja zagrożeń bezpieczeństwa informacji

Właściwe zdefiniowanie zagrożeń stanowi podstawę zapewnienia bezpieczeństwa informacji w przedsiębiorstwie. Zagrożenie to sytuacja lub stan, które komuś zagrażają lub w których ktoś czuje się zagrożony. Źródłem zagrożenia może być również osoba stanowiąca zagrożenie lub wzbudzająca poczucie zagrożenia[8]. „(…) W definicjach politologicznych, zwłaszcza odnoszących się do kwestii bezpieczeństwa, zagrożenia mieszczą się w szerszej grupie, określanej jako wyzwania. Wyzwania, które są właściwie rozpoznawane i podejmowane, stanowią szanse, zaś wyzwania nie podejmowane lub podejmowane za późno mogą przekształcić się w zagrożenia”[9]. Podobnie traktuje się zagrożenia również w innych naukach, takich jak na przykład zarządzanie czy socjologia.

Przedsiębiorstwa, których działania skupiają się na rozwoju i podążaniu w kierunku nowych rozwiązań, stają przed nowymi wyzwaniami i nowymi zagrożeniami, których katalog nieustannie się powiększa. Rysunek 2 prezentuje listę wybranych zagrożeń informacyjnych dla organizacji gospodarczej.

Prowadzenie działalności gospodarczej niesie za sobą ryzyko, które w przedsiębiorstwie pojawia się w postaci określonego zagrożenia. Ryzyko to przybiera różne formy i może ulegać zmianom w czasie. „(…) W refleksji nad niepewnością i ryzykiem w globalnym społeczeństwie informacyjnym należy ryzyko łączyć z zagrożeniami, a raczej kumulacją ryzyk wywodzących się z licznych źródeł zagrożeń (…)”[10].

2) Konieczny J., *O metodzie rozumowań w etyce bezpieczeństwa*, [w:] Konieczny J. (red.), *Bezpieczeństwo. Teoria i praktyka. Moralne problemy bezpieczeństwa*, czasopismo Krakowskiej Szkoły Wyższej im. A. Frycza Modrzewskiego, numer specjalny, Kraków 2008, s. 97.

3) Šmid W., *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000, s. 50.

4) Ciborowski L., *Walka informacyjna*, Wydawnictwo Marszałek, Toruń 1999, s. 186.

5) Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 71.

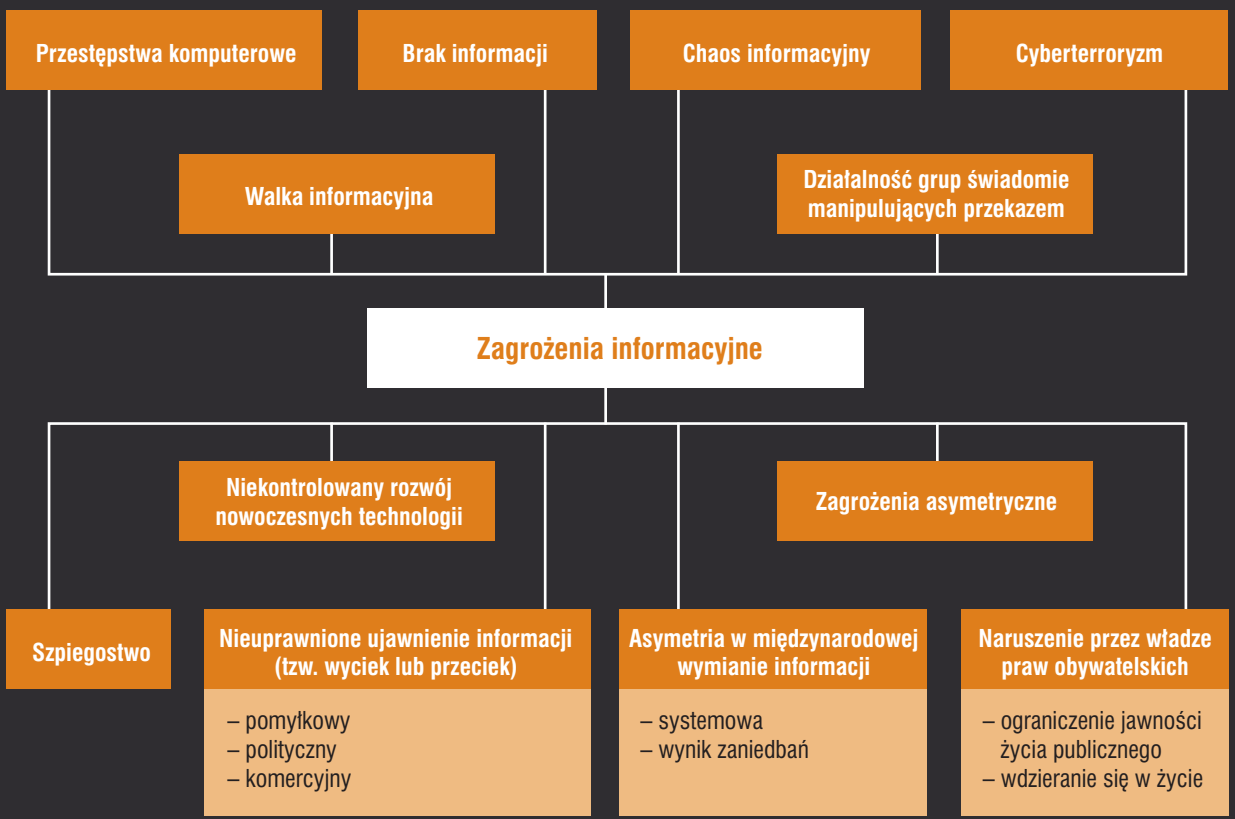
6) Tamże, s. 71.

7) Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Oficyna Współczesna, Poznań 2004, s. 80.

8) *http://sjp.pwn.pl/lista.php?co=zagro%BFenie* (data pobrania: 18 lipca 2008 r.).

9) Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30.

10) Sienkiewicz P., Społeczeństwo informacyjne jako społeczeństwo ryzyka, [w:] Haber L. W., Niezgoda M. (red.), Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006, s. 64.



Rys. 2. Podział zagrożeń informacyjnych
Źródło: Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30.

Wyróżniamy liczne źródła zagrożeń (ryzyka):
- ryzyko egzystencjalne,
- ryzyko kulturowe,
- ryzyko informacyjne,
- ryzyko technologiczne,
- ryzyko ekonomiczne,
- ryzyko ekologiczne,
- ryzyko polityczne,
- ryzyko...[11]

W przedsiębiorstwach spotykamy się z coraz większą skalą przestępstw i patologii gospodarczych. Tabela 1 przedstawia zagrożenia w biznesie w zakresie przestępstw gospodarczych, komputerowych i działalności wywiadów.

Przestępstwa występujące w biznesie tworzą specyficzną grupę, ponieważ, zagrażając przedsiębiorstwom czy instytucjom, stanowią zagrożenie dla zasobów organizacji, np. dla posiadanych baz informacji, środków pieniężnych, wartości firmy, takich jak reputacja, wyrobione stosunki bądź przywileje handlowe danego przedsiębiorstwa[12].

Pojęcie bezpieczeństwa informacyjnego można przybliżyć poprzez identyfikację następujących obszarów zagrożeń:
- zagrożenia losowe – wszelkiego rodzaju klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyjnego organizacji (np. pożar budynku, w którym przechowywane są nośniki informacji),
- tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyjna lub sabotażowa (ukierunkowana na zdobycie informacji, ofensywną dezinformację prowadzoną przez inne osoby, podmioty, organizacje),
- zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przechowywaniem, przetwarzaniem i przekazywaniem informacji w sieciach teleinformatycznych (do takich zagrożeń zaliczamy przestępstwa komputerowe, cyberterroryzm, walkę informacyjną),
- zagrożenia wynikające z niedostatecznych rozwiązań organizacyjnych i strukturalnych[13].

Zagrożenia można podzielić ze względu na lokalizację ich źródła na:
1. wewnętrzne (powstające wewnątrz organizacji), które obejmują:
   - zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu błędu lub przypadku,
   - zagrożenie utratą lub uszkodzeniem poprzez celowe działania nieuczciwych użytkowników,
2. zewnętrzne (powstające poza organizacją), które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu,
3. fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje z powodu wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe[14].

11) Tamże, s. 64.

12) Kuta M., *Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne*, [w:] Borowiecki R., Kwieciński M., *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze 2003, s. 268.

13) Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 72.

14) Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000, s. 65.

Przestępstwa w biznesie		
Gospodarcze i bankowe	**Komputerowe**	**Działalność wywiadów**
• fałszerstwa dokumentów publicznych (np. tożsamości, sprawozdań finansowych) • oszustwa: – kredytowe – prywatyzacyjne – podatkowe – celne – ubezpieczeniowe – upadłościowe – wyłudzenie towarów – „pranie pieniędzy” – inne	– niszczenie informacji – fałszerstwa danych – podsłuch – sabotaż – piractwo – wandalizm – *hacking* – *cracking*	– gospodarczego (wywiad technologiczny, handlowy, konkurencyjny, finansowy, strategiczny) – wojskowego – naukowego

Tab. 1. Przestępstwa w biznesie
Źródło: Kuta M., Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne, [w:] Borowiecki R., Kwieciński M., Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa, Zakamycze 2003, s. 267.

Jednym z najistotniejszych potencjalnych źródeł zagrożeń dla bezpieczeństwa przedsiębiorstw jest naruszanie przepisów ochraniających te organizacje przez osoby posiadające dostęp do informacji. Napotyka się również bariery i trudności związane z wdrażaniem w życie ustawy o ochronie informacji niejawnych.

Rozwój teleinformatyki i globalnego rynku automatyzuje procesy produkcyjne i finansowo–księgowe, umożliwia globalną i szybką komunikację, a nawet pozwala na zawieranie umów między kontrahentami na odległość. Jednakże nie należy zapominać o tym, że prowadzenie działalności gospodarczej w oparciu o teleinformatyzację oprócz korzyści niesie za sobą różne zagrożenia. Systemy informatyczne mają na celu gromadzenie, przetwarzanie i szybkie udostępnianie danych. „Wielkość ich i jakość, a zwłaszcza źródło pochodzenia stanowią przedmiot zainteresowania nie tylko służb specjalnych i innych instytucji będących potencjalnym przeciwnikiem, ale także organizacji o charakterze terrorystycznym oraz pojedynczych osób”[15]. Systemy informatyczne mogą być zagrożone ze strony każdego, kto posiada dostateczny zasób wiedzy i umiejętności.

Bezpieczeństwo systemów i sieci teleinformatycznych „to taki zakres przedsięwzięć, który ma na celu uniemożliwienie niepowołanym osobom dostępu do wartościowej informacji, do której można dotrzeć przez przechwyt emisji radiowych i analizę ruchu w sieciach radiowych lub wprowadzenie w błąd tych, którzy takową analizę mogą prowadzić. Bezpieczeństwo systemów łączności obejmuje systemy transmisji, bezpieczeństwo środków utrudniających oraz środków mających na celu fizyczną ochronę systemów łączności, materiałów niejawnych i informacji związanych systemami łączności”[16].

Ataki na zbiory danych stanowiących tajemnicę państwową lub służbową mają na celu przejęcie kontroli nad chronionymi systemami. Ataki na systemy komputerowe występują wówczas, gdy działania zmierzające do naruszenia ich bezpieczeństwa są celowe. Wyróżnia się dwie grupy ataków:

1. ataki aktywne – aktywne oddziaływanie na system, bezpośrednie lub pośrednie, polegające na modyfikowaniu strumienia danych lub tworzeniu danych fałszywych,
2. ataki pasywne – brak aktywnego oddziaływania na system (do ataków tych należy szeroko rozumiany podsłuch lub podgląd, analiza ruchu w sieci w celu zlokalizowania takich elementów, jak serwer czy stanowiska pracy)[17].

Zagrożenie atakiem występuje, gdy dostępne są takie możliwości, jak:

1. nieuprawniony dostęp do przechowywanych, przetwarzanych i przesyłanych informacji niejawnych bez oddziaływania na system,
1. nieuprawnione oddziaływanie na system, które może spowodować:
   – zmiany funkcjonowania sieci teleinformatycznej, dostęp do przesyłanych, przetwarzanych i przechowywanych informacji,
   – dezinformację,
   – zniszczenie informacji i innych zasobów systemu,
   – sfałszowanie lub nieuprawnioną modyfikację informacji[18].

W roku 2007 najczęściej pojawiającym się rodzajem ataku były oszustwa komputerowe, drugim pod względem liczebności rodzajem ataku były obraźliwe i nielegalne treści, natomiast na trzeciej pozycji uplasowało się gromadzenie informacji. Wciągu pięciu lat liczba ataków tego ostatniego rodzaju zmniejszyła się o 57%. Ponad połowa atakujących to firmy komercyjne (58,8%). Z roku na rok CERT Polska (Computer Emergency Response Team Polska) notuje coraz więcej takich przypadków. 18,5% atakujących pozostało nieznanych, w związku z czym przed organizacjami zajmującymi się ochroną pojawiają się coraz to nowe wyzwania. CERT często nie jest w stanie zidentyfikować prawdziwego źródła ataku, gdyż atakujący ukrywa sie za serwerem proxy, botnetem czy przejętą maszyną nieświadomej ofiary. Pojawiły się również i upowszechniły działające na granicy prawa firmy udostępniające łącza, serwery fizyczne i wirtualne, na których umieszczane są nielegalne treści, a firmy te chronią swoich klientów, zapewniając im anonimowość[19].

Najstarszą techniką mającą na celu wyprowadzenie danych z przedsiębiorstwa jest zbieranie przez konkurencję informacji o przedsiębiorstwie poprzez przeszukiwanie śmieci. Technika ta znajduje się na pograniczu zewnętrznego i wewnętrznego zagrożenia. Stanowi ona realne zagrożenie dla

15) Tamże, s. 63.

16) Herman M., *Potęga wywiadu*, Wydawnictwo Bellona, Warszawa 2002, s. 170.

17) Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000, s. 63.

18) Barczyk A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003, s. 70.

19) *http://www.cert.pl/PDF/Raport_CP_2007.pdf* (data pobrania: 14 lipca 2008 r.).

takich organizacji, jak banki, instytucje finansowe, ubezpieczeniowe, przedsiębiorstwa opracowujące i wdrażające nowe technologie, dla których poufność kontaktów z klientem jest podstawą zdobywania udziału w rynku. „O popularności tej techniki decyduje nie tylko łatwość, z jaką dane takie można zdobyć, lecz również – w przypadku zatrzymania – bezkarność”[20].

Ochrony wymagają nie tylko informacje związane z działalnością ekonomiczną i finansową, ale również dane osobowe. Przykładem luki w systemie ochrony danych osobowych może być fakt wykradzenia list z nazwiskami, adresami i numerami zastrzeżonych numerów telefonów ok. 200 tys. abonentów z baz danych piotrkowskiego oddziału TP (dane na płytach CD można było kupić na bazarze za 10 zł)[21].

„Rozwój technologii informacyjnych stwarza dogodne warunki dla prowadzenia działalności przestępczej. Pojawiające się nowe rozwiązania z jednej strony wspomagają procesy podejmowania decyzji na różnych szczeblach zarządzania organizacją, natomiast z drugiej niosą ze sobą jakościowo nowe niebezpieczeństwa. Zagrożenia te mogą naruszać zasoby: osobowe, materialne, finansowe, informacyjne (…)”[22]. Poniższa ilustracja przedstawia formy działań charakterystycznych dla przestępstw informatycznych.

Wyzwaniem dla przedsiębiorstw jest zapewnienie tajności, spójności i niezawodności działań związanych z gromadzeniem, przetwarzaniem i udostępnianiem danych wyłącznie uprawnionym osobom, co wynika z zajmowanego przez nie stanowiska lub wykonywania powierzonych im zadań. Wymienia się pięć obszarów zagrożeń dla systemów komputerowych:

- kwalifikacje i wiarygodność personelu,
- centra administracyjne systemu i sieci,
- infrastruktura telekomunikacyjna,
- produkcja sprzętu i oprogramowania,
- procedury korzystania z systemów i sieci informatycznych,
- nośniki danych[23].

Mając świadomość tego, jak wiele istnieje zagrożeń bezpieczeństwa informacji, należy wyselekcjonować najistotniejsze potencjalne obszary ich występowania. Trzeba opracować i wdrożyć procedury mające na celu ochronę tych obszarów, wprowadzić procedury ograniczające (uprawniony) dostęp, przeprowadzić szkolenia oraz kontrolować.

3. Podsumowanie

W pierwszej części niniejszego artykułu poruszono zagadnienia związane z istotą bezpieczeństwa informacji i klasyfikacją związanych z tym bezpieczeństwem zagrożeń. Część druga będzie poświęcona kształtowaniu zachowań zabezpieczających informacje w małej firmie.

dr Marek Jabłoński
Uniwersytet Ekonomiczny w Krakowie

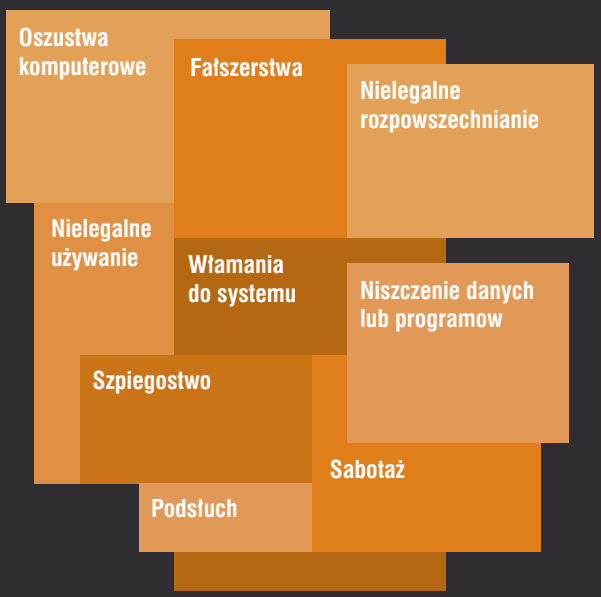
mgr Magdalena Mielus
Krakowska Szkoła Wyższa
Im. A. Frycza Modrzewskiego

20) Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Oficyna Współczesna, Poznań 2004, s. 45.

21) *http://www.wiadomosci.tvp.pl* (wiadomość z dnia 20 kwietnia 2003 r.).

22) Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000, s. 70.

23) Tamże, s. 64.



Rys. 3. Rozkład i nakładanie się przestępstw komputerowych
Źródło: Fischer B., Przestępstwa komputerowe i ochrona informacji, Kantor Wydawniczy Zakamycze, Zakamycze 2000, s. 33.

Literatura:

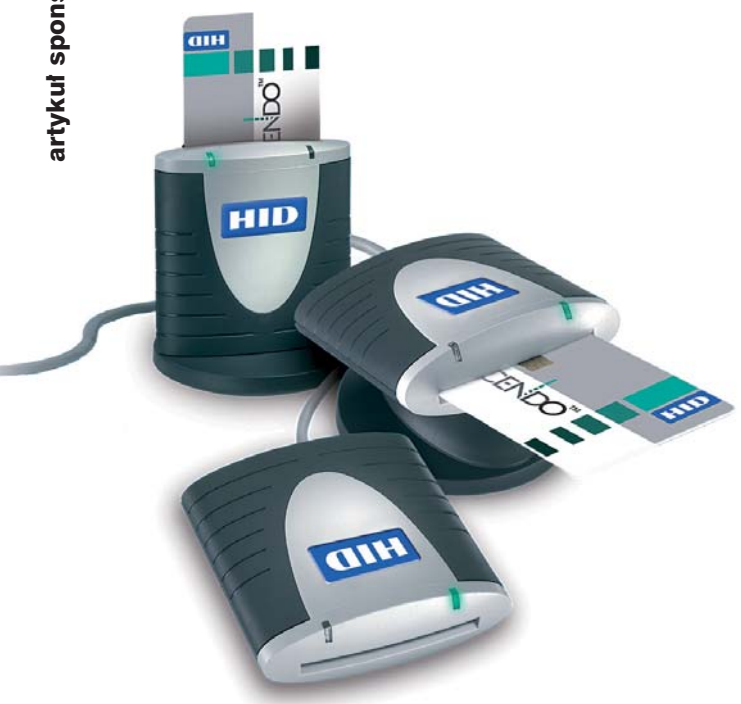
1. Barczyk A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003.
2. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.
3. Konieczny J. (red.), *Bezpieczeństwo. Teoria i praktyka. Moralne problemy bezpieczeństwa*, czasopismo Krakowskiej Szkoły Wyższej im. A. Frycza Modrzewskiego, numer specjalny, Kraków 2008.
4. Borowiecki R., Kwieciński M., *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze 2003.
5. Ciborowski L., *Walka informacyjna*, Wydawnictwo Marszałek, Toruń 1999.
6. Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kantor Wydawniczy Zakamycze, Zakamycze 2000.
7. Herman M., *Potęga wywiadu*, Wydawnictwo Bellona, Warszawa 2002.
8. Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006.
9. Šmid W., *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000.
10. Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Oficyna Współczesna, Poznań 2004.
11. Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000.

Źródła internetowe:

1. *http://sjp.pwn.pl*
2. *http://www.cert.pl*

Crescendo

– jedna karta, a tak wiele możliwości



Świat kontroli dostępu zmienia się zasadniczo. Także HID Global, uznany lider światowy w zakresie bezpiecznej identyfikacji, wykonał następny krok, oferując rozwiązania łączące w sobie zarówno fizyczną, jak i logiczną kontrolę dostępu. *– Firmy są obecnie bardziej świadome ważności kwestii bezpieczeństwa w otaczających nas aplikacjach ze świata informatyki* – powiedział Czesław Półtorak, dyrektor sprzedaży w HID Global Polska. *– Poprzez opracowanie Crescendo HID Global wypełnił lukę w kontroli dostępu, dostarczając bezpieczne jednokartowe rozwiązanie, łączące zarówno fizyczną, jaki i logiczną kontrolę dostępu*

Kontrola dostępu do aplikacji informatycznych opierała się wyłącznie na nazwach użytkowników i hasłach, jednakże, w związku ze wzrostem stopnia rozpowszechnienia tych aplikacji w miejscu pracy, wielu pracowników musi teraz pamiętać nawet tuzin zestawów nazw użytkowników i haseł, które są niewygodne w użyciu. Ludzie często zapominają swoich danych uwierzytelniających, co powoduje, że nie mogą wykonywać swojej pracy. Co gorsza, niektórzy sfrustrowani pracownicy mogą zdecydować się na zapisywanie swoich haseł, co zwiększa prawdopodobieństwo, że zostaną one skradzione lub wykorzystane w sposób nieautoryzowany. Bezpieczeństwo bazujące tylko na hasłach jest powszechnie uważane za słabą metodę uwierzytelniania, gdyż polega na czymś, co się wie.

Microsoft silnie promuje uwierzytelnianie poprzez karty chipowe jako preferowaną metodę logowania się do systemów informatycznych, gdyż rozwiązanie to zapewnia dwa składniki uwierzytelniania – „coś, co się posiada" (czyli kartę chipową) i „coś, co się wie" (czyli kod PIN albo hasło przypisane do tej karty). Poprzez używanie tej samej karty i kombinacji haseł w celu uzyskania dostępu do aplikacji informatycznych logowanie się użytkownika staje się wygodniejsze i wyeliminowana jest potrzeba pamiętania wielu haseł.

Karta Crescendo z HID Global jest identyfikatorem pracownika przenoszącym uwierzytelnianie do następnego poziomu – poprzez zapewnienie bezpiecznego dostępu zarówno do systemów informatycznych, jak i do budynków. Większość pracowników korzysta już z identyfikatorów pozwalających im na wstęp na teren zakładu pracy. Tradycyjnie są to identyfikatory ze zdjęciem, które pokazuje się przy wejściu głównym do budynku. – *W ciągu ostatnich 15–20 lat wiele firm zdecydowało się stosować bezpieczne bezstykowe karty i czytniki, takie jak iCLASS czy HID Prox, w celu zapewnienia fizycznej kontroli dostępu do drzwi* – powiedział Półtorak. *– Dzięki używaniu Crescendo wielu użytkowników rzeczywiście docenia korzyści, jakie płyną z posiadania jednej karty, która zapewnia im zarówno dostęp fizyczny, jak i logiczny*.

Oprócz zapewnienia dostępu do budynku bezstykowe karty HID Global mogą być wykorzystane w wielu zastosowaniach, takich jak kontrola dostępu do parkingów, rejestracja czasu pracy, płatności elektroniczne czy bezpieczne drukowanie sieciowe z serwerami wydruku w systemie *pull printing*. Wiele z takich aplikacji zostało opracowanych dzięki światowej sieci HID Connect Partners, która przyczynia się do zwiększania funkcjonalności i wartości technologii HID dla użytkownika końcowego.

Przedstawiciel VMC House, dostawcy bezgotówkowych rozwiązań płatniczych z Wielkiej Brytanii, dodał, że użytkownicy Crescendo mogą na swoje karty „załadować wartość", używając „ładowarek do pieniędzy elektronicznych". Taka karta może następnie zostać użyta do zakupów w automatach, płatności w restauracjach lub dowolnych terminalach płatniczych (POS) zlokalizowanych na terenie przedsiębiorstwa czy obiektu, w którym pracują. Technologia bezgotówkowa zapewnia także dodatkowe korzyści, takie jak obniżone koszty obsługi gotówki, szybsze czasy transakcji, powodujące znaczne skrócenie czasu spędzonego w kolejce do kasy w stołówce, większa wygoda, gdyż użytkownicy nie muszą pamiętać o noszeniu gotówki na drobne zakupy, a także lepsza higiena, jako że monety nie są już potrzebne, co jest szczególnie ważne np. w środowisku szpitalnym.

W karcie Crescendo można także wykorzystać rozmaite technologie bezstykowe. Pozwala to na używanie tej samej karty Crescendo do uzyskiwania dostępu do wielu różnych budynków, nawet wtedy, gdy zastosowane są różne

technologie dostępu fizycznego. Nie trzeba wymieniać przy tym zastosowanych wcześniej czytników.

Aby ułatwić zapewnienie bezpieczeństwa systemów informatycznych, w karcie Crescendo zawarte jest stykowe rozwiązanie, które zapewnia kryptografię Infrastruktury Klucza Publicznego (PKI – ang. *Public Key Infrastructure*). PKI to metoda wymiany informacji i bezpiecznej komunikacji w systemach informatycznych. Polega ona na użyciu pary kluczy – prywatnego i publicznego – zapisanych w certyfikatach cyfrowych, które są w sposób unikatowy przypisane do indywidualnych użytkowników w celu zapewnienia bezpiecznej komunikacji i dostępu. Przez wykorzystanie PKI w Crescendo możliwe jest zaszyfrowanie dokumentów i podpisanych cyfrowo wiadomości, takich jak e-mail, w taki sposób, że nadawca i odbiorca mogą być pewni, że komunikacja nie została zniszczona, odczytana czy zmieniona w jakikolwiek sposób, co pozwala im na współpracę, interakcje i dokonywanie transakcji *on-line* w sieci w bezpieczny i pewny sposób.

Aplikacje Microsoftu, takie jak Word, Excel, Power Point i Exchange, rutynowo wspierają inteligentne karty takie jak Crescendo, które zostały też certyfikowane przez Microsoft do pracy z oprogramowaniem Microsoft Identity Lifecycle Manager 2007. – *Oprócz używania kart Crescendo do logowania się do komputera można także użyć ich do zabezpieczania dostępu do poufnych dokumentów MS Word, takich jak umowy prawne czy zamówienia, a także do kontroli zmian danych finansowych czy danych klientów w arkuszach MS Excel* – powiedział Czesław Półtorak.

Inne aplikacje wspierane przez Crescendo obejmują zabezpieczenia dostępu do VPN, systemów pojedynczego logowania i rozwiązań uwierzytelniania przed załadowaniem systemu (ang. *pre-boot authentication*). Dodatkowe korzyści z używania kart Crescendo wynikają z tego, że są one dostosowane do współpracy z wiodącymi systemami fizycznej kontroli dostępu i systemami informatycznymi. – *Z uwagi na to, że referencja użytkowników jest zapisana na inteligentnej karcie, ten unikatowy wzorzec jest przenośny i może być przenoszony gdziekolwiek tam, gdzie się znajdą. Oznacza to, że możliwe jest uwierzytelnienie i przyznanie odpowiednich praw dostępu do budynków firmowych albo aplikacji informatycznych nawet wtedy, gdy użytkownik pracuje w różnych miejscach, podróżuje albo wykonuje swą pracę w domu* – powiedział Półtorak. – *HID zadbał o to, aby zastosowanie kart Crescendo było tak łatwe, jak tylko jest to możliwe. Jeszcze niedawno temu PKI uważano za rozwiązanie nieco tajemnicze i niewiarygodnie skomplikowane, kosztowne i czasochłonne w wykorzystywaniu. Dzięki poczynionym przez Microsoft postępom w ułatwianiu zastosowania PKI jesteśmy w stanie dostarczać karty Crescendo ze standardowymi ustawieniami, które są odpowiednie do wielu zastosowań. Zdecydowaliśmy się także umieścić nasze oprogramowanie pośredniczące (ang. middleware) na karcie, aby użytkownik nie musiał płacić oddzielnie za oprogramowanie i zajmować się skomplikowanymi umowami licencyjnymi.*

Źródło: HID Global
tłumaczenie: Adam Bułaciński, Redakcja

Biometria z NOVUSA

część 1

Dotychczas firma NOVUS znana była w branży zabezpieczeń elektronicznych głównie z produktów przeznaczonych do monitoringu wizyjnego, rejestracji cyfrowej sygnałów wizyjnych oraz oprogramowania integrującego. W ostatnim okresie firma postanowiła rozszerzyć swój asortyment o produkty przeznaczone do systemów kontroli dostępu – i to od razu o te z najwyższej półki, wykorzystujące biometryczne metody identyfikacji użytkownika

Urządzenia biometryczne w Polsce

Z miesiąca na miesiąc przybywa na polskim rynku produktów przeznaczonych do systemów kontroli dostępu, które wykorzystują do identyfikacji użytkownika jego cechy biometryczne. Na razie dominują urządzenia wyposażone w skanery odcisku palca, chociaż pojawiają się już ciekawe produkty wyposażone w kamerę, która umożliwia identyfikację użytkownika na podstawie kształtu twarzy czy wzoru tęczówki oka. Jak w przypadku większości produktów na rynku, o ich sukcesie marketingowym decyduje w pierwszej kolejności cena. Obecnie najtańsze są urządzenia bazujące na skanerach odcisku palca. Ich cena zbliża się do ceny, po jakiej jeszcze niedawno oferowane były zwykłe czytniki zbliżeniowe. To decyduje o ich rosnącej popularności. Pozostałe wspomniane wcześniej rozwiązania są aktualnie co najmniej kilka razy droższe.

Wracając do urządzeń wykorzystujących skanowanie palca, zalecam potencjalnym użytkownikom i instalatorom dużą ostrożność przy wyborze sprzętu, który zamierzają nabyć i użytkować. Aktualna oferta rynkowa w zakresie czytników i kontrolerów biometrycznych obejmuje szeroki asortyment produktów, które na pierwszy rzut oka wyglądają podobnie i mają bardzo zróżnicowane ceny (od kilkuset złotych do kilku tysięcy za sztukę).

Z użytkowego punktu widzenia najważniejsze są parametry funkcjonalne. I właśnie tym parametrom należy poświęcić najwięcej uwagi przy wyborze produktu, bowiem często jest tak, że bardzo podobnie wyglądające urządzenia oferują zupełnie różne, często bardzo znaczące funkcje. Największe szanse trwałego zaistnienia na rynku mają urządzenia, które są bardzo elastyczne funkcjonalnie, co umożliwia ich różnorakie wykorzystanie.

Do takiej grupy urządzeń można niewątpliwie zaliczyć kontroler biometryczny o symbolu NVAC-C300CKF firmy NOVUS.

Co to jest NVAC-C300CKF?

Urządzenie o symbolu NVAC-C300CKF to zaawansowany technologicznie kontroler biometryczny o dużych możliwościach funkcjonalnych i aplikacyjnych. W skrócie można określić go, parafrazując znaną reklamę, jako „5 w 1”. Co takiego kryje w sobie to urządzenie?

Oto odpowiedź:

- sterownik kontroli dostępu (kontroler),
- optyczny skaner odcisku palca,
- czytnik kart zbliżeniowych w standardzie L lub H,
- klawiaturę cyfrową z przyciskami funkcyjnymi,
- graficzny wyświetlacz LCD.

Wszystkie te podzespoły zostały zintegrowane w jednej estetycznej obudowie przystosowanej do montażu na ścianie. Schemat blokowy urządzenia przedstawia rysunek 1.

Poszczególne komponenty kontrolera NVAC-C300CKF realizują następujące funkcje:

1. Wyświetlacz LCD – dwuliniowy, typu graficznego, wyświetla komunikaty systemowe zarówno w trybie użytkowym, jak i w trybie programowania. Dzięki temu, że jest to wyświetlacz typu graficznego, możliwe jest wyświetlanie dowolnych czcionek, ponieważ urządzenie oferuje menu w wielu językach. Wyświetlacz ma dwa tryby pracy: z podświetleniem lub bez. Pierwszy tryb jest domyślnie włączany podczas programowania lub podczas identyfikacji użytkownika. Może być również włączony na stałe. Drugi tryb jest trybem energooszczędnym i jest domyślnie włączony w stanie spoczynku. W stanie spoczynku na wyświetlaczu prezentowana jest aktualna data i godzina. Po zaprogramowaniu może być wyświetlana również, jako napis stały lub przesuwany, nazwa firmy klienta. Po pozytywnej weryfikacji użytkownika wyświetlany jest komunikat powitalny, który może zawierać nazwisko lub identyfikator użytkownika.

2. Klawiatura cyfrowa – zawiera standardową 12-polową klawiaturę numeryczną oraz cztery przyciski funkcyjne. Przyciski cyfrowe służą do wprowadzania kodu ID oraz do wpisywania wartości w trybie programowania. Przyciski funkcyjne od F1 do F4 służą do poruszania się po menu w procesie programowania. Przyciski te w przyszłości będą służyć również do realizacji funkcji związanych z rejestracją czasu pracy.

3. Czytnik kart zbliżeniowych – pod obrazem karty na obudowie urządzenia zlokalizowany jest czytnik kart zbliżeniowych. Aktualnie, w zależności od wersji anteny, urządzenie obsługuje karty pracujące na częstotliwości 125 kHz (wersja L) lub 13,56 MHz (wersja H). W wersji L możliwy jest odczyt popularnych kart typu UNIQUE lub HID ISO PROX. W wersji H czytnik odczytuje karty w technologii Mifare Philips lub iClass HID 2k. Pod tym względem jest to bardzo unikatowe urządzenie na naszym rynku. Informacja o odczytanym numerze karty jest przesyłana do kontrolera, który wysyła ją między innymi na wyjście Wieganda w formacie 26, 34 lub 64 bity. W trybie programowania urządzenie może pełnić rolę czytnika administratora i służyć do wpisywania numerów kart do pamięci urządzenia.

4. Skaner odcisku palca – typu optycznego, z zewnątrz przysłonięty jest szybką, którą można łatwo czyścić. Pod dolną krawędzią skanera zlokalizowany jest czujnik przyłożenia palca. Dzięki temu możliwe jest włączenie skanera i szybki dostęp tylko przez przyłożenie palca.

Po załączeniu skanera zapala się podświetlenie w kolorze czerwonym – jest to oznaka procesu skanowania. Skanowanie może być jedno- lub wielokrotne. Jest to bardzo ważny element całego urządzenia, ponieważ wraz z algorytmem procesu skanowania decyduje w dużym stopniu o poziomie

Rys. 1. Schemat blokowy kontrolera NVAC-C300CKF

bezpieczeństwa, jaki oferuje kontroler. W trybie programowania skaner może pełnić rolę czytnika administratora i służyć do wpisywania wzorców do pamięci urządzenia.

5. Sterownik kontroli dostępu – w pełni funkcjonalny kontroler analogiczny do rozwiązań stosowanych w standardowych systemach kontroli dostępu. Integruje wszystkie opisane powyżej elementy w jedną funkcjonalną całość. Oprócz tego posiada następujące złącza:

- Port Wieganda (WE) umożliwiający podłączenie drugiego czytnika kart zbliżeniowych,
- Port Wieganda (WY) umożliwiający podłączenie do zewnętrznego kontrolera,
- Port RS232, wielofunkcyjny,
- Port TCP do współpracy z programem administracyjnym,
- 3 wejścia linii dozorowych,
- 2 wyjścia przekaźnikowe.

W kontrolerze jest zawarty program producenta (*firmware*) oraz pamięć bazy danych i pamięć zdarzeń.

Jak działa kontroler biometryczny NVAC-C300CKF?

Jak wspomniałem wcześniej, urządzenie jest bardzo elastyczne i może pracować w różnych konfiguracjach funkcjonalnych. Można wyróżnić trzy podstawowe tryby pracy urządzenia:

1. tryb autonomiczny – jako samodzielny sterownik, który steruje zamkiem elektrycznym poprzez jedno z wyjść przekaźnikowych;
2. tryb Master/Slave – jako zintegrowany czytnik biometryczno-zbliżeniowy współpracujący z zewnętrznym kontrolerem innego producenta (np. Kantech, RBH) poprzez wyjście Wieganda;
3. tryb sieciowy – jako element rozległego systemu, w którym kontrolery są monitorowane i zarządzane poprzez program nadzorczy NAM (urządzenie ma własny programowany adres IP).

W trybie autonomicznym i sieciowym, w zależności od przyjętego sposobu kontroli przejścia – jedno- lub dwustronnej, może zaistnieć potrzeba dołączenia dodatkowych urządzeń do kontrolera NVAC-C300.

Przykładowe konfiguracje

1. Kontrola dwustronna (wejście/wyjście) – dwa kontrolery NVAC-C300. Taka konfiguracja gwarantuje najwyższy poziom bezpieczeństwa. Oba kontrolery połączone są ze sobą łączem cyfrowym (RS232), a sterowanie zamkiem elektrycznym odbywa się z przekaźnika kontrolera wewnętrznego.

2. Kontrola dwustronna (wejście/wyjście) – jeden kontroler NVAC-C300 od strony wejścia i standardowy czytnik kart zbliżeniowych (np. NVAC100/200) od strony wyjścia (wejście – KARTA & PALEC, wyjście – tylko KARTA). Do sterowania zamkiem elektrycznym zaleca się w tym przypadku zastosowanie specjalnego modułu bezpieczeństwa, który jest zlokalizowany wewnątrz strefy chronionej (np. w obudowie zasilacza buforowego) i połączony z kontrolerem NVAC-C300 łączem cyfrowym (RS232). Moduł ten zawiera dwa przekaźniki – drugi przekaźnik może być wykorzystany do wysterowania syreny alarmowej w przypadku sabotażu zewnętrznego kontrolera biometrycznego.

3. Kontrola jednostronna (tylko wejście) – jeden kontroler NVAC-C300 od strony wejścia. Ze względów bezpieczeństwa zaleca się w tym przypadku zastosowanie do sterowania zamka elektrycznego modułu bezpieczeństwa zlokalizowanego wewnątrz strefy chronionej i połączonego łączem cyfrowym z kontrolerem zewnętrznym. Jeżeli istnieje konieczność zainstalowania przycisku wyjścia od strony wewnętrznej, to należy go również dołączyć do odpowiedniego wejścia modułu bezpieczeństwa.

Pod względem metody identyfikacji użytkownika kontroler może pracować w jednym z 11 trybów. Lista tych trybów zawiera różne kombinacje trzech metod identyfikacji poprzez:

- odcisk palca,
- kartę zbliżeniową,
- kod ID.

Przykładowe tryby to np. tryb gwarantujący najwyższe bezpieczeństwo – ID & KARTA & PALEC (należy użyć kolejno kodu PIN, karty i palca) lub mieszany – ID & PALEC albo KARTA & PALEC (w którym wystarczy użyć, odpowiednio, kodu PIN i palca albo karty i palca).

Na uwagę zasługują również takie funkcje, jak:

- *antipassback*, czyli kontrola przejścia powrotnego (dla konfiguracji dwustronnej, zapobiegająca powtórnemu wejściu bez uprzedniego wyjścia),
- dostęp po pozytywnej weryfikacji dwóch użytkowników,
- dyskretny alarm po wejściu „pod przymusem” (dyskretny kod wejścia).

Niezbędny do prawidłowego działania urządzenia proces programowania urządzenia może się odbywać na jeden z dwóch sposobów:

- lokalnie, z wykorzystaniem zintegrowanej klawiatury i wyświetlacza (dostęp do menu zabezpieczony jest hasłem biometrycznym),
- zdalnie, poprzez sieć TCP albo RS232, za pomocą programu NAM, z którego jest dostęp do centralnej bazy danych.

Pierwsza opcja jest wystarczająca w przypadku pojedynczych urządzeń, druga jest zalecana dla dużych, rozproszonych systemów. Również w przypadku wykorzystania urządzenia jako zintegrowanego czytnika biometryczno-zbliżeniowego podłączonego do zewnętrznego kontrolera konieczne jest zaprogramowanie poszczególnych urządzeń poprzez sieć TCP.

Podsumowanie

Niniejszy artykuł nie opisuje oczywiście wszystkich szczegółów funkcjonalnych urządzenia. Zainteresowanych czytelników odsyłam jak zwykle do dokumentacji dostępnej na stronie www.aat.pl lub na nośniku CD, który można otrzymać w siedzibie firmy AAT.

Kartę katalogową kontrolera zawierającą szczegółowe dane techniczne znajdą Państwo na 79. stronie bieżącego numeru.

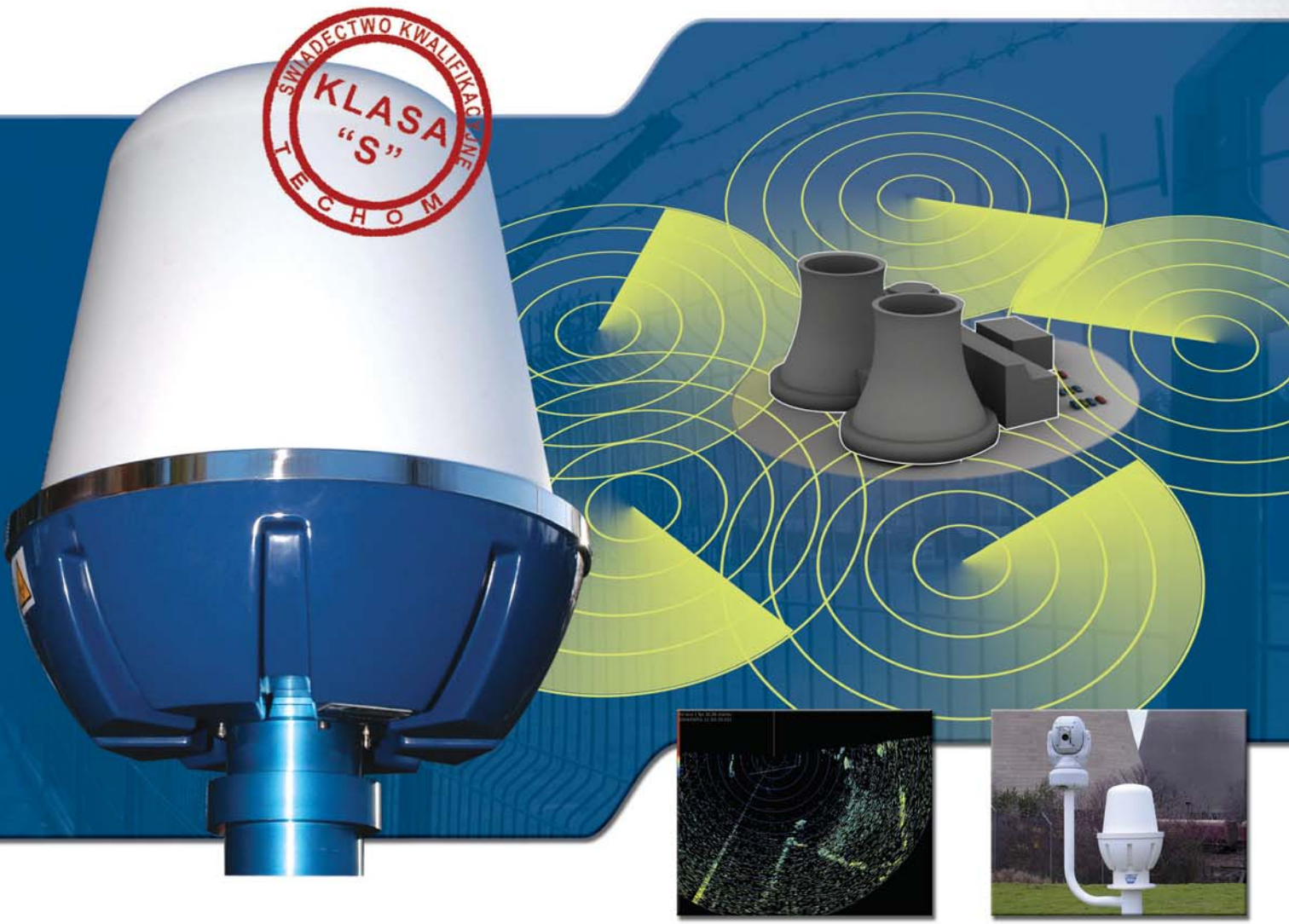
W jednym z kolejnych numerów *Zabezpieczeń* ukaże się artykuł opisujący program nadzorczy Novus Access Manager (NAM) przeznaczony do zarządzania siecią złożoną z wielu kontrolerów NVAC-C300CKF.

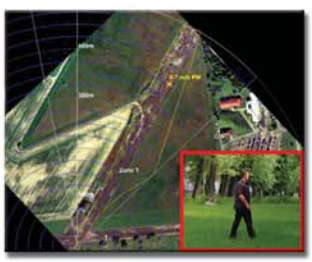
W bieżącym roku planowane jest również dalsze rozszerzenie funkcjonalności kontrolera o możliwość rejestracji czasu pracy (RCP) i generowanie związanych z tą funkcją raportów. Zagadnienia te będą również tematem następnego artykułu w jednym z kolejnych numerów.

Ryszard Sobierski
AAT Holding

KABE

WYZNACZAMY NOWE GRANICE OCHRONY





Nasze systemy radarowe wykrywają każde wtargnięcie osób i pojazdów na chroniony obszar, stale monitorując aktualną pozycję intruza. Radary automatycznie sterują zespołem kamer tworząc w pełni zintegrowany system ochrony.

KABE Sp. z o.o.
ul. Waryńskiego 63, 43-190 Mikołów
tel. 032 32 48 900 • fax 032 32 48 901
handel@kabe.pl • www.kabe.pl

Bezpieczeństwo aplikacji biznesowych

część 2
Infrastruktura i oprogramowanie

W pierwszej części artykułu przedstawiono aspekty związane z bezpieczeństwem aplikacji biznesowych w odniesieniu do bezpieczeństwa sieci. Niniejsza część jest poświęcona bezpieczeństwu infrastruktury oraz oprogramowania – w tym bezpieczeństwu systemu operacyjnego i bazy danych, na której działają aplikacje, oraz wewnętrznym mechanizmom zabezpieczającym, osadzonym już w samych aplikacjach

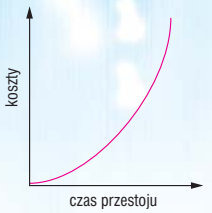
Bezpieczeństwo infrastruktury

Bardzo ważnym zagadnieniem związanym z bezpieczeństwem infrastruktury, na której uruchomione są aplikacje biznesowe, jest ich wysoka dostępność (w skrócie HA – *High Availability*). Jest ona wymagana, aby zwiększyć dostępność aplikacji z punktu widzenia użytkownika końcowego.

Wysoka dostępność aplikacji jest czymś więcej niż „dostępność" infrastruktury technicznej, ponieważ:
- redukuje planowane przerwy, występujące np. podczas tworzenia kopii zapasowych, aktualizacji, wgrywania poprawek,
- implementuje scenariusze odtwarzania awaryjnego, minimalizując skutki awarii,
- podwyższa poziom SLA (ang. *Service Level Agreement* – umowa o poziomie świadczenia usługi).

Dzięki podwyższeniu dostępności można także minimalizować „nieplanowane przestoje", które są wynikiem awarii sprzętowych, awarii aplikacji, błędów operatorskich, kataklizmów itp. zdarzeń. Aby dobrze zaplanować wysoką dostępność, należy zbadać wszystkie tak zwane pojedyncze punkty awarii (ang. *Single Point of Failures* – SPOF) i w odpowiedni sposób je zabezpieczyć.

Koszty przestoju nie są liniowe, rosną w czasie. Podczas długotrwałych przestojów koszty rosną progresywnie. Przykład: gdy proces SCM (ang. *Supply Chain Management* – zarządzanie łańcuchem dostaw) ma przestój dłuższy niż trzy godziny, cała produkcja staje, co znacząco podwyższa koszty prowadzenia działalności.



Rys. 1. Rozkład kosztów przestoju w czasie

W zapobieganiu przestojom pomocne są:
- zdublowanie komponentów (zabezpieczenie przed pojedynczymi punktami awarii),
- centrum zapasowe (na przykład w technologii klastrowej),
- narzędzia do zarządzania (odpowiednie oprogramowanie jest w stanie monitorować krytyczne komponenty i ostrzegać przed awarią),
- zespół IT (doświadczony zespół IT jest w stanie sprawnie reagować i zapobiegać awariom),
- planowanie zasobów (odpowiednie planowanie jest w stanie zabezpieczyć krytyczne zasoby),
- gwarantowane SLA (odpowiednie umowy są w stanie gwarantować odpowiedni poziom usług i wsparcia w razie awarii),
- proaktywne usługi.

Aby w pełni sprawnie realizować obsługę wysokiej dostępności, można korzystać z pomocy dostawców platformy sprzętowej, jak również systemu operacyjnego. Przykładami produktów, które to umożliwiają, mogą być:
- Microsoft Cluster Service (MSCS),
- HP Service Guard,
- SUN Cluster,
- Veritas Cluster Server,
- ORACLE Failsafe, ORACLE RAC,
- IBM HACMP.

Należy również pamiętać o podwyższeniu dostępności:
- sprzętu wewnętrznego (zasilaczy, wentylatorów itp.),
- rozwiązań składujących dane,
- elementów sieciowych (i rozkładaniu ich obciążenia).

Rozwiązania HA są oferowane przez dostawców sprzętu i wymagają dodatkowych usług lub konsultacji.

Dostępność	Przestój w tygodniu	Tygodniowe przestoje (przykłady)	Przestój w roku	Roczny przestój używany do ...	
99,9999 %	0,6 s	?	30 s	?	
99,9990 %	6 s	Tygodniowe testy przełączenia	5 min	Roczny restart (?)	
99,9900 %	1 min	Dzienne przełączenie	52 min	Jednoroczne wyłączenie aplikacji	Obecnie stosowane
99,9000 %	10 min	Tygodniowy restart	8h 45 min	Jeden backup off-line w roku	
99,0000 %	1 h 40 min	Zarządzanie off-line aplikacją	87 h 30 min		
90,0000 %	16h 48 min	Jeden backup off-line w tygodniu	36 dni		

Tab. 1. Skala wysokiej dostępności

Pojedynczy punkt awarii (SPOF)	Techniczne możliwości SPOF
Centralna baza danych	– Środowisko przełączalne
Centralne usługi	– Środowisko przełączalne – Konfiguracja serwera rozdzielającego
Centralne systemy plików	– Dzielenie plików w klastrze – Dzielenie plików przez NFS – Bazujące na sprzęcie środowisko wysokodostępne (RAID, inne)

Tab. 2. Możliwości eliminacji pojedynczych punktów awarii

Następujące kryteria determinują wybór rozwiązania HA:
- **stopień funkcjonalności HA (w szczególności SPOF)** – czy wszystkie SPOF są zabezpieczone i wyeliminowane, jak dużo z nich pozostało?
- **implementacja** – ile czasu zajmie wdrożenie rozwiązania HA?
- **wykrywanie „przełączenia"** – jak oprogramowanie klastrowe wykryje, że należy przełączyć zasoby?
- **czas przełączenia** – ile czasu potrzeba, aby po przełączeniu wszystkie zasoby powróciły?
- **liczba potrzebnych maszyn** – ile serwerów (maszyn) potrzeba, aby zaimplementować rozwiązanie HA?
- **architektoniczna otwartość i rozwijalność** – czy rozwiązanie HA jest rozwijalne i możliwe do wykorzystania w przyszłości?

Wysoka dostępność jest wynikiem współpracy dostawcy sprzętu, oprogramowania i klienta. Należy redukować pojedyncze punkty awarii poprzez stosowanie komponentów nadmiarowych, co prowadzi do minimalizacji przestojów. Wszystkie krytyczne komponenty (takie jak baza danych czy serwer aplikacyjny) powinny być zabezpieczone. Można obniżać planowane wyłączenia poprzez odpowiednie procedury.

Innym aspektem bezpieczeństwa infrastruktury jest stworzenie odpowiedniego centrum tworzenia kopii zapasowych wszystkich komponentów programowych aplikacji biznesowej, od systemu operacyjnego do samej aplikacji.

Bezpieczeństwo systemu operacyjnego i bazodanowego

Bardzo ważny ze względu na bezpieczeństwo aplikacji biznesowej jest system operacyjny, w którym jest ona uruchomiona. Każdy system operacyjny posiada swoją specyfikę i powinno się go należycie zabezpieczyć i wzmocnić (*OS hardening*). Wzmacnianie systemu polega na eliminacji zbędnych usług wewnętrznych i sieciowych, zastosowaniu najnowszych poprawek i aktualizacji aplikacji, które w nim są uruchomione. Powinno się stosować zasadę: „co nie jest dozwolone, jest zabronione".

Obecnie najczęściej używane są dwa typy systemów:
- Windows Server,
- Unix/Linux/BSD.

W systemach Windows należy zadbać przede wszystkim o:
- użytkowników i ich uprawnienia,
- uprawnienia do systemu plików,
- dostęp z zewnątrz (konsola),
- ochronę współdzielonych zasobów,
- usługi katalogowe i domeny,
- ochronę pamięci dzielonej,
- ochronę antywirusową.

W systemach typu Unix należy zadbać o:
- użytkowników i ich uprawnienia,
- uprawnienia do systemu plików,
- dostęp z zewnątrz (SSH) (konsola),
- ochronę współdzielonych zasobów.

Następnym bardzo ważnym komponentem jest baza danych. Większość obecnie używanych aplikacji wiodących producentów używa baz danych (np. Oracle, SAP, Microsoft, TETA, Comarch).

Baza danych jest **krytyczna** dla takich aplikacji i bez niej nie są one w stanie działać, dlatego na jej zabezpieczenia należy zwrócić odpowiednio dużą uwagę.

Najczęściej używane bazy danych to:
- Oracle,
- MS SQL,
- DB2/Informix,
- mySQL.

Każda baza danych ma specyficzne zabezpieczenia, jednak ze standardowych mechanizmów należy zwrócić uwagę na:
- użytkowników dostępowych do bazy danych,
- dostęp do samej bazy danych (zdalny/lokalny),
- uprawnienia do plików bazy danych,
- *backup/restore*.

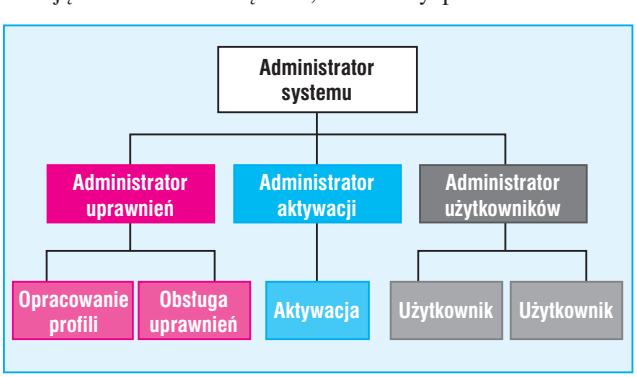
Baza danych, jak również system operacyjny, na którym uruchamiana jest aplikacja biznesowa, są bardzo ważnymi komponentami w budowaniu całościowych mechanizmów związanych z bezpieczeństwem. Błąd w zabezpieczeniu dowolnego z tych komponentów może skutkować skompromitowaniem aplikacji biznesowej.

Role i mechanizmy wbudowane w samej aplikacji

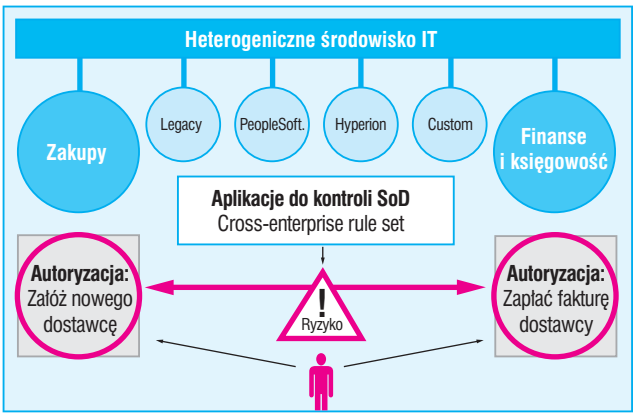
Każda aplikacja posiada własny wewnętrzny mechanizm zarządzania rolami i uprawnieniami.

Obecnie w aplikacjach biznesowych jest dużo tematów, które wiążą się z wnętrzem aplikacji. Wyzwania, z jakimi mamy do czynienia, to:
- powszechne ryzyko podziału obowiązków,
- kosztowna ręczna eliminacja słabych punktów,
- niekontrolowane zarządzanie rolami,
- nadmierny dostęp administratora,
- nieskuteczna i nieaudytowalna obsługa użytkownika,
- kosztowne podejście reakcyjne w kontekście zapobiegania naruszaniu bezpieczeństwa.

Rozdział obowiązków (ang. *Segregation of Duty* – SoD) jest obecnie tematem bardzo ważnym z punktu widzenia audytów zewnętrznych i zgodności z SOX. Aplikacje, które kontrolują rozdział obowiązków, chociażby pakiet SAP GRC



Rys. 2. Mechanizm zarządzania rolami i uprawnieniami w aplikacji biznesowej



Rys. 3. Przykład działania aplikacji wykrywającej konflikt w uprawnieniach

Access Control, umożliwiają kontrolę uprawnień od strony biznesowej i posiadają wbudowaną macierz konfliktów.

Na rysunku 3 pokazano działanie aplikacji wykrywającej konflikt w uprawnieniach na przykładzie osoby, która z jednej strony może dokonywać zamówień u dostawców zewnętrznych, jak również może ich dodawać, a z drugiej ma możliwość akceptacji pochodzących od nich faktur.

Z drugiej strony niektóre aplikacje posiadają swoje wewnętrzne mechanizmy kontroli i audytu (kto wystawił fakturę, kto ją zmienił itp.) oraz mechanizmy logowania zdarzeń. Ważna jest też ochrona plików aplikacji, które są przechowywane w systemie plików. Jeżeli te pliki są krytyczne (jak np. logi), to można ustawić opcję ich natychmiastowego wydruku. W takim przypadku intruz nie jest już w stanie fizycznie ich zmienić.

Podsumowanie

Obecnie wiele firm prowadzi działania związane z bezpieczeństwem typu „zamek średniowieczny", zabezpieczając się poprzez firewalle, skanery antywirusowe itp. Bezpieczeństwo rozdziela się w tym przypadku na „wewnętrzne" i „zewnętrzne". Przewaga takiego podejścia to: łatwość instalacji i administracji, duża niezależność od aplikacji, jasno zdefiniowane koszty. Ma ono jednak również wady:

a) brak ochrony przed nowoczesnymi zagrożeniami
   – ciągły wyścig pomiędzy atakami a technologiami ochrony
   – potrzeba kooperacji z wykorzystaniem metod coraz potężniejszych, lecz potencjalnie bardziej narażonych na ataki (XML, Web Services itp.)

b) ograniczenia w rozszerzeniu
   – miasta rozszerzają się, przekraczając dawne granice
   – biznes rośnie ponad stare granice

c) zbyt duża liczba restrykcji w handlu międzynarodowym.

Z tego powodu należy pamiętać, że **nie można żadnego systemu zabezpieczyć w 100%**, ponieważ występują błędy ludzkie (popełniane w rozwoju oprogramowania, przy konfiguracji systemu, podczas jego obsługi). Zabezpieczenie pojedynczego systemu często jest zbyt drogie. Dlatego należy zawsze stosować mieszane rozwiązania i podejście zdroworozsądkowe.

JACEK BUGAJSKI
SID GROUP

POLON-ALFA

Największy polski producent systemów sygnalizacji pożarowej

POLON-ALFA

Zakład Urządzeń Dozymetrycznych Sp. z o.o.
85-861 Bydgoszcz, tel. 052 36 39 261, fax 052 36 39 264
www.polon-alfa.pl

Podsystemy diagnostyczne

w systemach sygnalizacji włamania i napadu (część 2)

W pierwszej części artykułu omówiona została geneza podsystemów diagnostycznych oraz związane z nimi postanowienia normy PN-EN-50131-1:2007. Poniżej przedstawiono zaawansowane podsystemy diagnostyczne, stosowane głównie w SSWiN o strukturze rozproszonej

Podsystemy diagnostyczne

Pierwsze podsystemy diagnostyczne zastosowane w SSWiN miały niewielkie możliwości i ich zadanie ograniczało się do określania poziomu napięcia zasilania głównego (czyli napięcia zmiennego, które w owym czasie miało wartość 220 V). W przypadku jego braku następowało przełączenie na źródło zasilania rezerwowego, jakim jest akumulator. Wymusiło to konieczność pomiaru także napięcia akumulatora i, w przypadku jego rozładowania, okresowego jego doładowywania.

Podsystemy diagnostyczne stosowane w systemach sygnalizacji włamania i napadu o strukturze skupionej, czyli takiej, w której wszystkie czujki linii dozorowych, manipulatory i sygnalizatory akustyczne lub optyczne są połączone bezpośrednio z płytą główną centrali alarmowej, umożliwiają określenie stanu systemu. Jeżeli system ma ochraniać obiekt o dużej powierzchni i liczbie stref, to zachodzi konieczność zastosowania SSWiN o strukturze rozproszonej, w której do centrali alarmowej podłączone są określone moduły. Moduł jest to układ dołączany do jednostki centralnej w celu realizacji ściśle określonych funkcji (np. zwiększenia liczby wejść lub wyjść, wzmocnienia prądowego magistral komunikacyjnych, współpracy z tablicami synoptycznymi, współpracy z komputerowym systemem rejestracji zdarzeń występujących w całym systemie oraz wykonywania programowo przewidzianych działań). Dlatego również podsystem diagnostyczny uległ modernizacji i zamiast stosować jeden scentralizowany układ kontrolno-pomiarowo-diagnostyczny, zaczęto projektować go w wersji rozproszonej. Stosuje się jeden nadrzędny układ odpowiedzialny za pracę podukładów, których zakres czynności diagnostycznych jest stosunkowo mały.

W systemach sygnalizacji włamania i napadu o strukturze rozproszonej, które mają nadzór komputerowy, stosuje się rozwiązania polegające na monitorowaniu wielu sygnałów diagnostycznych. Na ich podstawie sygnalizowany jest użytkownikowi stan „AWARIA" (przez diodę LED na manipulatorze rzeczywistym lub wirtualnym oraz wyświetlenie komunikatu na ekranie komputera nadzorującego pracę systemu – rys. 1).

W przypadku stosowania manipulatora osoba upoważniona może dokonać przeglądu występujących awarii. Zostało to pokazane na rys. 2.

Niezbędne jest także poinformowanie odpowiednich służb (np. serwisanta, konserwatora) w celu usunięcia niepożądanego stanu w systemie. Można wykorzystać w tym celu połączenie zdalne, np. poprzez sieć Internet czy GSM (pod warunkiem zapewnienia bezpieczeństwa przesyłu danych), jeśli projektant przewidział takie rozwiązanie. Umożliwia to serwisowi przeprowadzenie diagnostyki SSWiN „na odległość" i ocenę rodzaju awarii. Rys. 3 przedstawia widok okna „Awarie" programu komputerowego służącego do programowania i nadzoru systemu.

Możliwe jest też przeprowadzenie diagnostyki systemu w celu zweryfikowania jego prawidłowego działania (np. przez określenie poziomu napięć zasilania modułów). Na rys. 4 przedstawiono zobrazowanie pomierzonych wartości napięć zasilających moduły wraz ze strukturą przykładowego systemu.

Jeśli projektant systemu nie przewidział możliwości zdalnej diagnostyki, w niektórych typach SSWiN o strukturze rozproszonej możliwy jest odczyt pomierzonych napięć zasilających poszczególne moduły poprzez wykorzystanie manipulatora. Przedstawia to rys. 5 i 6.

Powyżej przedstawiono przykładowe możliwości podsystemów diagnostycznych. Podsumowując można dodać, że rozbudowane podsystemy diagnostyczne umożliwiają wykrycie m.in. następujących awarii:

- awarii ogólnej (sygnalizacja wykrycia stanu uszkodzenia),
- braku zasilania podstawowego płyty głównej centrali alarmowej,
- awarii akumulatora płyty głównej centrali alarmowej,
- braku akumulatora płyty głównej centrali alarmowej,
- braku zasilania podstawowego ekspandera [n], gdzie n – numer ekspandera,
- awarii akumulatora ekspandera [n], gdzie n – numer ekspandera,
- braku akumulatora ekspandera [n], gdzie n – numer ekspandera,
- awarii zasilania manipulatorów,
- awarii szyny ekspanderów,
- awarii szyny manipulatorów,
- braku zasilania podstawowego tablicy synoptycznej [n], gdzie n – numer tablicy synoptycznej,
- awarii akumulatora tablicy synoptycznej [n], gdzie n – numer tablicy synoptycznej,
- braku akumulatora tablicy synoptycznej [n], gdzie n – numer tablicy synoptycznej,
- awarii wyjścia [n], gdzie n – numer wyjścia centrali alarmowej,
- awarii, której sygnał jest doprowadzany z wejścia [n], gdzie n – numer wejścia,
- awarii baterii w urządzeniu bezprzewodowym [n], gdzie n – numer urządzenia bezprzewodowego,
- awarii zegara,
- braku sygnału DTR na porcie RS232,
- błędu inicjacji modemu,
- sytuacji, gdy odpowiedzią modemu na komendę AT jest „ERROR",
- braku napięcia na linii telefonicznej,

– występowania na linii telefonicznej sygnału przerywanego,
– braku sygnału na linii telefonicznej,
– problemu z transmisją do stacji monitorowania,
– braku kabla modułu Ethernet,
– awarii układu RTC,
– błędu sumy kontrolnej (CRC) danych centrali,
– braku manipulatora,
– zamiany manipulatora,
– braku ekspandera,
– zamiany ekspandera.

Niektóre z komunikatów dotyczących wymienionych wyżej awarii zaliczane są także do informacji o sabotażu części lub całości elementów i urządzeń systemu sygnalizacji włamania i napadu.

Wnioski

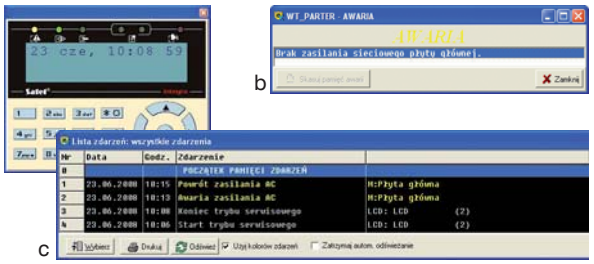
Stosowanie podsystemów diagnostycznych w systemach sygnalizacji włamania i napadu wydaje się w dzisiejszych czasach rozwiązaniem, które już przyjęło się wśród producentów, projektantów, instalatorów, użytkowników i serwisantów. Przyczynił się do tego bardzo szybki rozwój systemów mikroprocesorowych i komputerowych. Dzięki temu możliwy jest pomiar wielu wielkości ciągłych i dyskretnych występujących w systemie przy stosunkowo niskich kosztach takiego SSWiN. Jednocześnie zdalna diagnostyka pozwoliła na ograniczenie kosztów związanych z serwisem dzięki możliwości wykonania części czynności obsługowych „na odległość". Pracownicy serwisu, jadąc do uszkodzonego systemu, mają pełniejszą wiedzę na temat tego, w jakim stanie eksploatacyjnym się on znajduje, co jest uszkodzone i jakie elementy czy urządzenia należy mieć ze sobą w celu dokonania naprawy lub obsługi. Pozwala to na wyraźne zmniejszenie nakładów finansowych przeznaczonych na personel serwisowy, a także ogranicza wydatki związane z transportem elementów niezbędnych do naprawy, gdyż mogą one zostać wcześniej zamówione i zabrane przez pracowników.

Wydaje się, że rozwój podsystemów diagnostycznych stosowanych w SSWiN będzie postępował w kierunku dalszego zwiększania liczby monitorowanych parametrów z uwzględnieniem możliwości ich podglądu poprzez sieć telekomunikacyjną. Należy także sądzić, że będą wprowadzane komputerowe programy wspomagające podejmowanie decyzji eksploatacyjnych, które umożliwią optymalizację kosztów związanych z przeglądami okresowymi SSWiN.

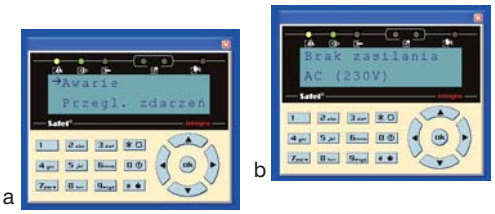
DR INŻ. ADAM ROSIŃSKI

Literatura

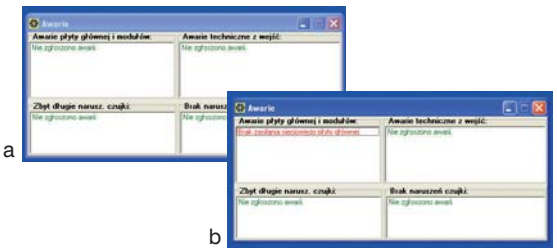
1. Będkowski L., Dąbrowski T., *Podstawy eksploatacji, cz. II. Podstawy niezawodności eksploatacyjnej*, Wojskowa Akademia Techniczna, Warszawa 2006.
2. Instrukcje serwisowe i użytkowników systemów GALAXY, RANKOR, SATEL.
3. Korbicz J., Kościelny J., Kowalczuk Z., Cholewa W., *Diagnostyka procesów. Modele. Metody sztucznej inteligencji. Zastosowania*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002.
4. Rosiński A., *Proces odnowy systemów nadzoru, w: Prace naukowe Politechniki Radomskiej* nr 2(20)/2004, Radom 2004.



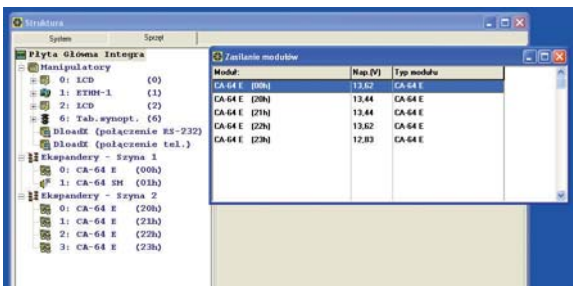
Rys. 1. Przykłady złożonego systemu diagnostycznego stosowanego w SSWiN z nadzorem komputerowym i sygnalizacją uszkodzenia: a)z wykorzystaniem wirtualnego manipulatora, b)poprzez komunikat, c)poprzez listę zdarzeń



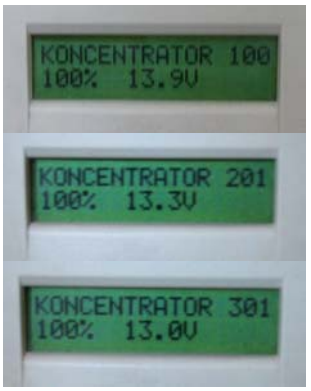
Rys. 2. Przegląd rodzajów uszkodzeń z wykorzystaniem wirtualnego manipulatora: a)wybór funkcji przeglądu awarii, b)określenie rodzaju awarii



Rys. 3. Widok okna „Awarie": a)w przypadku braku awarii, b)w przypadku braku zasilania podstawowego płyty głównej centrali alarmowej

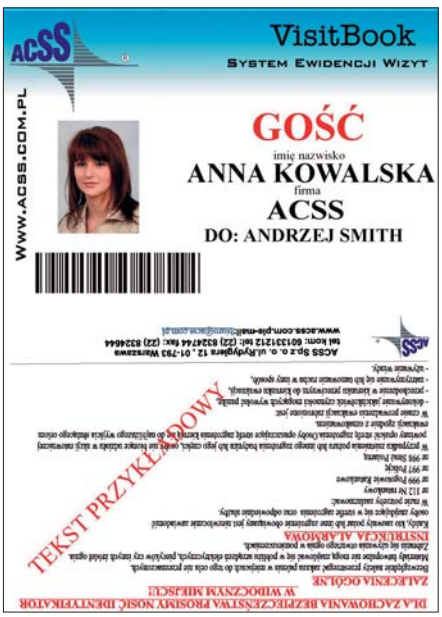


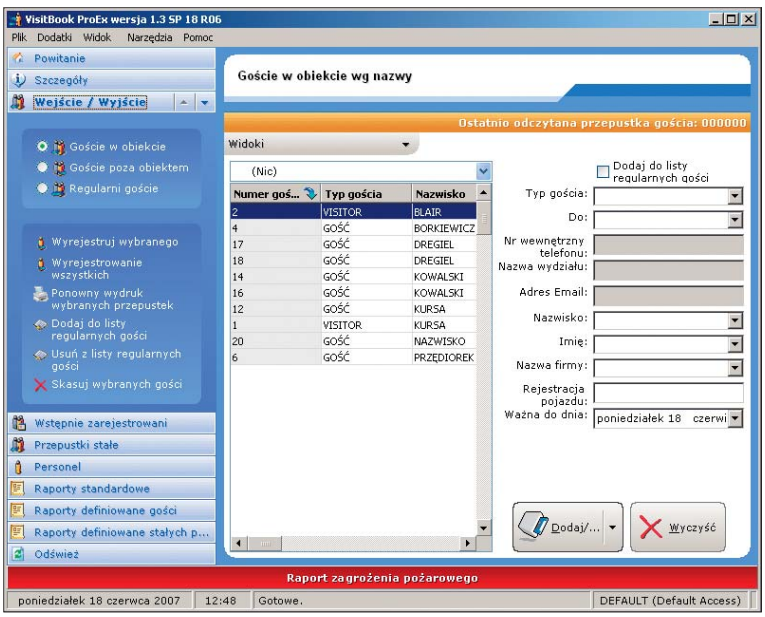
Rys. 4. Struktura systemu i wartości napięć zasilających moduły



Rys. 5. (z lewej) Wybór opcji diagnostycznych poprzez manipulator
Rys. 6. (z prawej) Wartości napięć na poszczególnych modułach systemu

System rejestracji gości VisitBook





Wybrane funkcje systemu VisitBook	wersja LITE	wersja PRO	wersja PRO EX	wersja xFR
Kontrola gości, Kontrahentów, Personelu	tak	tak	tak	tak
Rejestracja wstępna	–	tak	tak	tak
Lista regularnych gości	–	tak	tak	tak
Pobieranie zdjęcia	–	–	tak	tak
Czytnik kodów kreskowych	–	tak	tak	tak
Elektroniczny podpis	–	–	tak	tak
Przepustka pojazdu	–	–	tak	tak
Drukowanie na PVC	–	–	tak	tak
Format bazy danych	Access	Access	Access	MSSQL / MySQL
Dostępność w sieci	–	tak	tak	tak
Administracja konferencji/ wystaw	–	–	tak	tak
Własne wzory przepustek	–	–	tak	tak
Raport standardowy	tak	tak	tak	tak
Raporty definiowane	–	tak	tak	tak
Zabezpieczenie sprzętowe	klucz USB	klucz USB	klucz USB	klucz USB

System rejestracji gości VisitBook jest narzędziem służącym do wspomagania pracy recepcji. Zastępuje papierową księgę gości – jest jej elektronicznym odpowiednikiem. System umożliwia rejestrację danych osób odwiedzających budynek wraz z wydrukiem ich przepustek. Proces wydruku przepustki gościa oraz przechwycenia jego zdjęcia jest płynny i szybki. Rejestrację wejścia i wyjścia gościa można zautomatyzować stosując czytnik kodów kreskowych. Program VisitBook jest dostępny w czterech wersjach: Lite, Pro, ProEx i xFR.

Wersja Lite pozwala na drukowanie przepustek z podstawowymi danymi personalnymi, a rejestracji wejść i wyjść dokonuje pracownik recepcji.

Wersja Pro dodatkowo umożliwia nadruk na przepustce kodu kreskowego wykorzystywanego przy automatycznej rejestracji wejść/wyjść.

ProEx jest wersją bardziej rozbudowaną w porównaniu do wcześniejszych. Umożliwia wydruk przepustki wraz ze zdjęciem i zawiera m.in. funkcję projektowania własnych wzorów przepustek.

Podstawową zaletą różniącą czwartą wersję xFR od pozostałych jest zastosowana w niej platforma SQL zapewniająca szybkość i niezawodność obsługi dużych, ruchliwych obiektów.

Wydruk przepustek jest możliwy na standardowych drukarkach biurowych oraz drukarkach do kart PVC (tylko wersja Pro-Ex i xFR). Główną zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym, np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program ponadto zawiera kilka użytecznych funkcji, takich jak: manager personelu, manager kontrahentów, obsługa konferencji.

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
http://www.acss.com.pl

Inteligentny tester akumulatorów GOLD-IBT

GOLD-IBT

inteligentny tester akumulatorów

Producenci akumulatorów zalecają wymianę akumulatora, jeżeli jego współczynnik pojemności spada poniżej 65%. Typowym miernikiem można zmierzyć tylko napięcie akumulatora.

Jak zmierzyć jego pojemność?

Inteligentny Tester Akumulatorów GOLD-IBT w kilka sekund dokonuje symulacji pełnego rozładowania akumulatora.

Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.

- Testuje w ciągu kilku sekund akumulatory wykonane w technologii AGM (elektrolit uwięziony w separatorach z włókna szklanego) – powszechnie używane w systemach alarmowych i UPS.
- Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.
- Cyfrowo zaprogramowany do pomiaru szczelnych akumulatorów (SLA) 12 V oraz akumulatorów samochodowych o pojemności od 1,2 Ah do 200 Ah.
- Testuje akumulatory szybko, dokładnie i jest łatwy w użyciu.

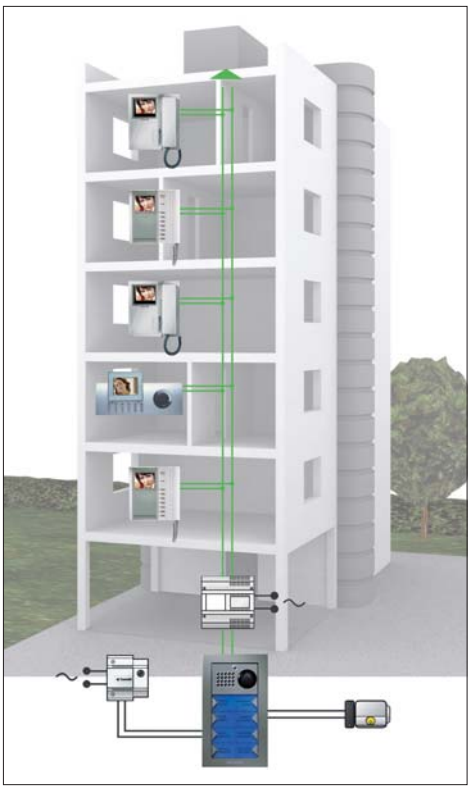
Dane techniczne	
Model	GOLD-IBT
Zasilanie	12 V DC (10-15 V DC)
Typ akumulatora	szczelne akumulatory (SLA) 12 V oraz akumulatory samochodowe
Pojemność akumulatora	1.2 Ah – 200 Ah
Symulowany test rozładowania akumulatora	C20 do 10,50 V DC @ 25°C
Wyświetlacz	podświetlany LCD
Pomiar temperatury	0°-100°C
Ostrzeżenie o zbyt wysokim napięciu	> 15 V DC
Ostrzeżenie o zbyt niskim napięciu	< 10 V DC
Ostrzeżenie o zbyt niskiej pojemności	< 0.5 Ah
Tolerancja pomiaru Ah	10% (zależy od konstrukcji i parametrów produkcyjnych akumulatora)
Zabezpieczenie temperaturowe odwrócenia polaryzacji	dioda blokująca
Zdolność wykonania kolejnych testów	do 15 następujących bezpośrednio po sobie
Ostrzeżenie przed przegrzaniem	> 55°C ± 10°
Wymiary	111 mm x 55 mm x 35 mm
Długość przewodów przyłączeniowych	40 cm
Masa w opakowaniu	400 gramów
Zawarte akcesoria	futerał, certyfikat zgodności, etykiety na akumulatory
Gwarancja	1 rok

alarmnet®

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
http://www.alarmnet.com.pl

2-przewodowy, kolorowy system wideodomofonowy firmy COMELIT



SBC SIMPLEBUS COLOR

Cechy systemu:

- kolorowe monitory z ekranami LCD;
- 2 przewody łącznie z zasilaniem monitora;
- 4 magistrale na zasilacz (np. 4 piony w budynku mieszkalnym);
- do 8 monitorów z funkcją interkomu na każdy apartament;
- do 240 użytkowników;
- do 600 m maksymalnej odległości pomiędzy panelem wejściowym, a ostatnim monitorem;
- nieograniczona liczba paneli głównych i dodatkowych;
- centralny moduł portiera;
- proste programowanie za pomocą przełączników;
- możliwość tworzenia systemów mieszanych audio i wideo;
- funkcja dzwonka lokalnego;
- oddalona sygnalizacja wywołania;
- programowalny moduł przekaźnikowy sterowany przyciskiem monitora bądź wybranym zdarzeniem w systemie;
- moduł kamer zewnętrznych;
- interfejs sygnału wideo do postaci analogowej;
- nowy, bezsłuchawkowy monitor PLANUX (dostępny w 9 kolorach).

Monitory wewnętrzne dostępne w systemie Simplebus Color

GENIUS

BRAVO

DIVA

PLANUX

Panele wejściowe

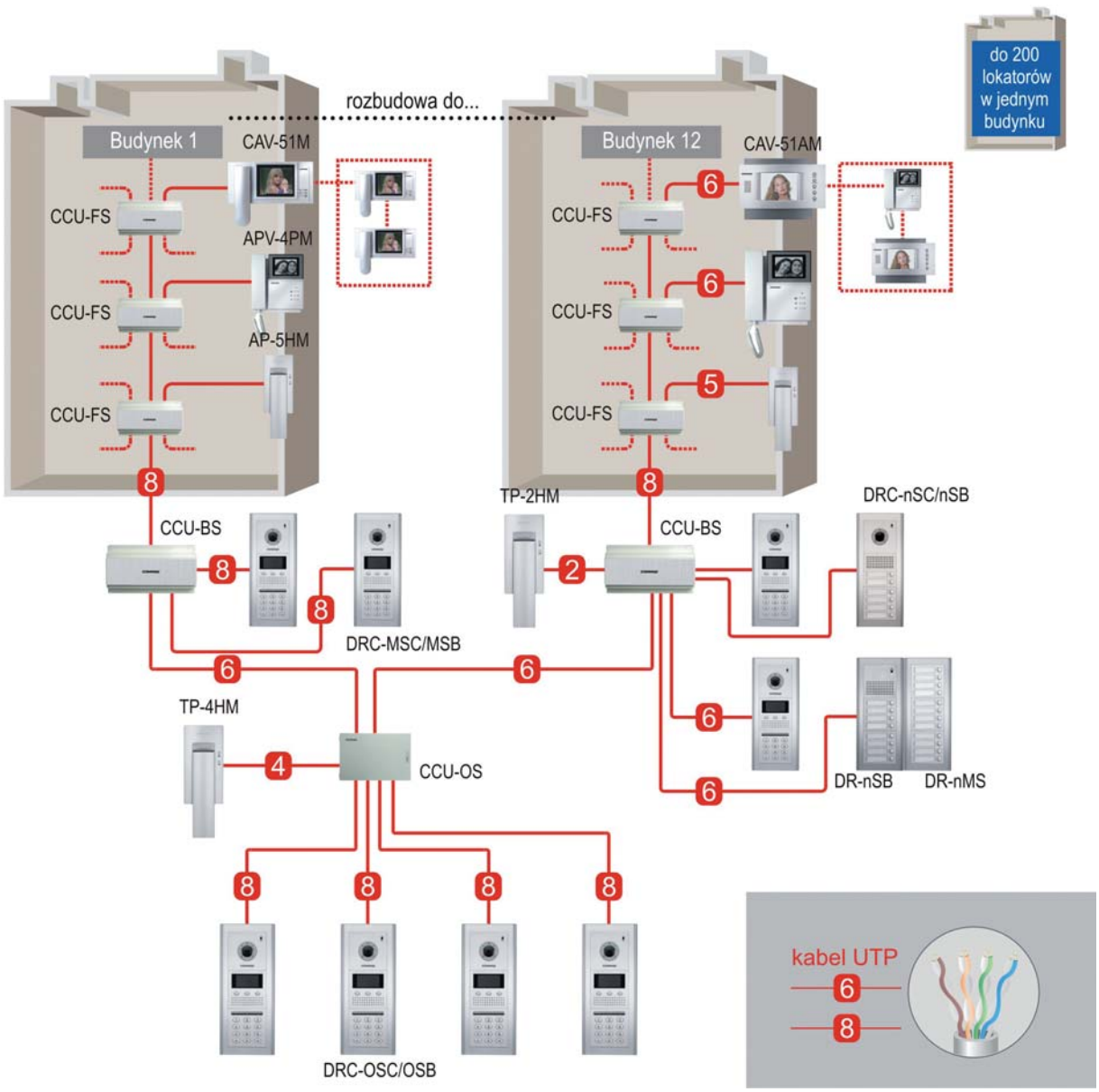
W systemie Simplebus2 można zastosować panele wejściowe serii Powercom jak i wandaloodporne Vandalcom. Oba panele występują w wersji cyfrowej z elektronicznym spisem nazwisk oraz z indywidualnymi przyciskami wywołania. Ramki zewnętrzne paneli dostępne są w różnych kolorach.

alarmnet®

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
http://www.alarmnet.com.pl

System wieloabonentowy serii 2400



System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna ilość obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu Slave).

Lokator może mieć zainstalowany prosty unifon, umożliwiający kontakt głosowy z osobą odwiedzającą jak i monitor (czarno-biały lub kolorowy), pozwalający także na obserwację wizualną osoby odwiedzającej.

System umożliwia zastosowanie zarówno paneli zewnętrznych audio, jak video - wyposażonych w moduł kamery (czarno-biały lub kolorowy). Panele zewnętrzne występują w wersji przyciskowej lub z klawiaturą numeryczną (umożliwiającą dodatkowo wybór lokatora za pomocą spisu lokatorów oraz otwieranie zamka elektrycznego przy użyciu indywidualnych kodów).

System może być wyposażony w unifon instalowany w portierni, przez co lokatorzy mogą mieć kontakt z osobą dozorującą (portierem). Dzięki dużej elastyczności możliwe jest skonfigurowanie systemu dla małych, pojedynczych bloków jak i całych osiedli zamkniętych, gdzie ogrodzonych może być klikanaście budynków, a całość nadzorowana przez kilku portierów.

GDE POLSKA
GLOBAL DISTRIBUTOR OF ELECTRONICS

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

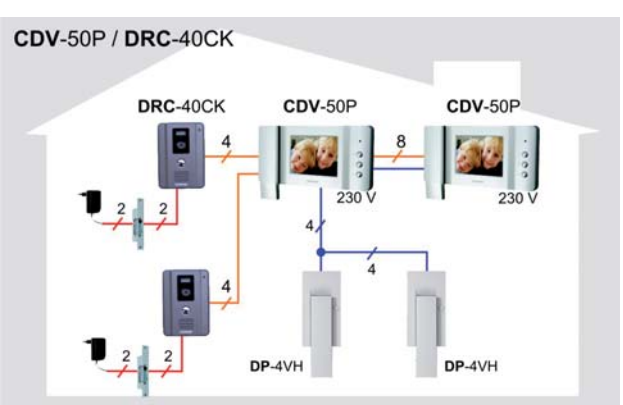
tel./faks (12) 256 50 35, 256 50 25
faks (12) 270 56 96
e-mail: biuro@gde.pl

Monitor CDV-50P i kamera DRC-40CK

Dane techniczne – Monitor CDV-50P	
Zasilanie	AC 100 V ~ 240 V 50 / 60 Hz
Pobór mocy	maks. 16 W
Monitor	5" Color TFT LCD
System kodowania obrazu	NTSC
Okablowanie	4 przewody do kamery
Podgląd obrazu	90 s (przy rozmowie) / 60 s (przy wywołaniu)
Temperatura pracy	od 0°C do + 40°C
Wymiary	258 x 159 x 51 mm (szer. / wys. / gł.)
Masa	0,85 kg

GDE POLSKA wprowadza na rynek polski nowy wideodomofon koreańskiego koncernu COMMAX. Urządzenie wyposażone jest w 5-calowy monitor, a wygląd zewnętrzny odróżnia się zdecydowanie od sprzętu innych firm. Wraz z kamerą DRC-40CK tworzy ciekawą propozycję dla osób, które chcą wyposażyć swój dom w niezawodny, a przy tym niedrogi wideodomofon. Monitor ma możliwość podłączenia drugiego panelu z kamerą, co umożliwia obsługę dwóch wejść na posesję. Wewnątrz budynku system wideodomofonowy może być rozbudowany o dodatkowe monitory lub same unifony, umożliwiające kontakt głosowy z wejściami (funkcja domofonu). Po rozbudowie systemu istnieje możliwość nawiązania łączności pomiędzy monitorami lub unifonami (funkcja interkomu).

Dane techniczne – Kamera DRC-40CK	
Zasilanie	DC 12 V (z monitora)
Przetwornik	CMOS
System kodowania obrazu	NTSC
Okablowanie	4 przewody monitor – kamery + zasilanie elektrozamka
Kąt widzenia	poziomy: 75°; pionowy: 55°
Czułość	0,1 lx (30 cm od soczewki)
Temperatura pracy	- 10°C ~ + 40°C
Wymiary	101 x 142 x 32 mm (szer. / wys. / gł.)
Masa	0,30 kg



Schemat połączenia CDV-50P/DRC-40CK

GDE POLSKA
GLOBAL DISTRIBUTOR OF ELECTRONICS

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

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

Kamera kolorowa kopułkowa z obiektywem ze zmienna ogniskową Falcon CC 280 Z

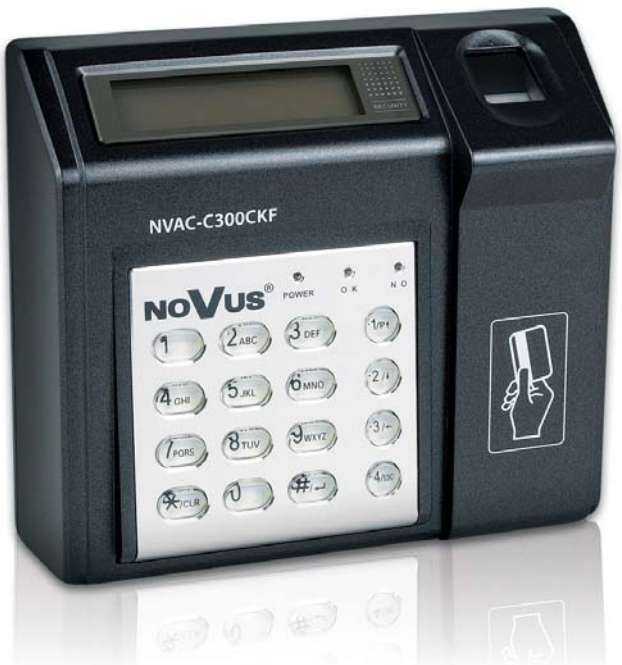
Kamera Falcon CC 280 Z otwiera nową linię urządzeń Falcon „Red Line" firmy Factor Security. Urządzenia te charakteryzują się wyższymi parametrami technicznymi, większym zakresem dostępnych opcji dzięki zastosowaniu japońskich podzespołów. CC 280 Z to kamera kopułkowa z przetwornikiem kolorowym 1/3" SONY Super HAD o rozdzielczości 530 lini. Główną zaleta kamery kopułowej jest zastosowany obiektyw wysokiej jakości o zmiennej ogniskowej 3,7-12 mm. Mimo niewielkich rozmiarów kamery zastosowany układ optyczny gwarantuje wysokiej jakości obraz wideo oraz pozwala na ustawienie obszaru obserwowanej sceny. Zastosowany obiektyw z automatyczna przysłoną predestynuje kamerę do pracy w zmiennych warunkach oświetlenia. Kamera oferuje także automatyczny balans bieli, automatyczną regulację wzmocnienia oraz kompensację światła tylnego. Kamera zasilana jest napięciem 12 V DC.

- przetwornik 1/3" CCD Super HAD SONY
- wysoka rozdzielczość pozioma – 530 TV linii
- zasilanie 12 V DC
- automatyczna regulacja wzmocnienia
- elektroniczna migawka
- automatyczny balans bieli
- kompensacja tła

Specyfikacja techniczna	
Przetwornik	1/3" CCD Super HAD SONY
Obróbka Sygnału	DSP
Rozmiar Matrycy	500 (H) x 582 (V)
Wielkość Matrycy	290000 px
Rozdzielczość Pozioma	530 TVL
Synchronizacja	Wewnętrzna
Skanowanie	2:1 z przeplotem
Czułość	0,5 lx / F2.0
Stosunek Sygnał/Szum	więcej niż 50 dB (przy AGC off)
Automatyczna Regulacja Czułości	TAK
Automatyczny Balans Bieli	TAK
Kompensacja JASNEGO TŁA	AUTO
Wyjście Wizyjne	1 Vp-p Composite Video, 75 Ω
Ogniskowa Obiektywu	regulowana: 3,7 – 12mm
Zasilanie	12 V DC ± 10%
Pobór Prądu	150 mA
Warunki Pracy	od -10°C do + 50°C / wilgotność do 70%
Wymiary (Śr. x Wys.)	107 x 86 mm
Masa	300 g

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
http://www.factor.pl

Kontroler biometryczny – NVAC-C300CKF



Budowa

Kontroler biometryczny (skaner palca) typu NVAC-C300CKF jest nowoczesnym urządzeniem wielofunkcyjnym przeznaczonym do pracy w systemach kontroli dostępu. Oprócz optycznego skanera linii papilarnych posiada zintegrowany czytnik zbliżeniowy kart Mifare/iClass lub HID/Unique, klawiaturę z przyciskami funkcyjnymi, graficzny wyświetlacz LCD oraz kontroler 1 przejścia (wyjście przekaźnikowe do sterowania zamkiem).

Dane techniczne kontrolera NVAC-C300CKF	
Pamięć odcisków	1910
Pamięć kart	4096
Pamięć transakcji	16000
FAR	0.00008 %
FRR	0.09 %
Rozmiar pamięci flash	1 MB
Porty komunikacyjne	Ethernet - złącze RJ-45, RS-232, Wiegand
Wejścia linii dozorowych	3
Wyjścia sterujące	2, przekaźnikowe
Typ czytnika kart	Wersja H 13,56 MHz (Mifare, iClass 2k) Wersja L 125 kHz (Unique, HID ISOPROX)
Sensor	Optyczny, 500 dpi
Rozmiar wzorca	256 - 384 bajty
Obszar detekcji skanera	16 (szer.) x 19 (wys.) mm
Sygnalizacja	3 diody LED
Zasilanie	12 V DC
Pobór mocy	11 W
Temperatura pracy	od 0°C do +50°C
Wymiary (mm)	147 (szer.) x 130 (wys.) x 51 (gł.)
Masa	550 g

Tryb pracy pod względem funkcjonalnym:

- autonomiczny (wyjście przekaźnikowe do sterowania zamka)
- sieciowy poprzez port Ethernet TCP/IP
- wyjście typu interfejs Wieganda 26/34 bity do współpracy z kontrolerami:
  - KT100, KT200 i KT300 i programami EntraPass firmy KANTECH
  - IRC2000, URC 2000 i programem INTEGRA32 firmy RBH
  - Kontrolerami innych producentów jeżeli mają porty Wieganda

Charakterystyka kontrolera NVAC-C300CKF

- Możliwość przypisania użytkownikowi 2 lub 4 wzorców odcisków palców
- Algorytm identyfikacji 1:1 lub 1: wielu
- 11 trybów pracy (kombinacje: palec, karta, kod)
- 12-polowa klawiatura numeryczna
- 4 przyciski funkcyjne F1 do F4
- Graficzny wyświetlacz LCD
- Przekaźnik do sterowania zamkiem elektrycznym
- Przekaźnik do uzbrajania systemu alarmowego
- 2 wejścia linii dozorowych
- Port do podłączenia czytnika wyjściowego
- Możliwość wyświetlania nazwiska użytkownika
- Możliwość wyświetlania nazwy firmy klienta
- Możliwość programowania przy pomocy klawiatury i wyświetlacza LCD lub programu na PC

AAT Holding sp. z o.o.
ul. Puławska 431
02-801 Warszawa

tel. (22) 546 05 46
faks (22) 546 05 01
http://www.aat.pl

2M ELEKTRONIK
ul. Majora 12a
31-422 Kraków
tel. (12) 412 35 94
faks (12) 411 27 74
e-mail: 2m@2m.pl
www.2m.pl

3D
Wielobranżowe Przedsiębiorstwo Sp. z o.o.
ul. Kościuszki 27C
85-079 Bydgoszcz
tel. (52) 321 02 77
faks (52) 321 15 12
e-mail: biuro@3d.com.pl
www.3d.com.pl

---

4 COM Sp. z o.o.
ul. Adama 1
40-467 Katowice
tel. (32) 609 20 30
faks (32) 609 20 30 wew. 103
e-mail: biuro@4.com.pl
www.4.com.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. 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

ADT POLAND Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 8 414
faks (22) 430 8 302
e-mail: adtpoland@tycoint.com
www.adt.pl

ALARM SYSTEM
Marek Juszczyński
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

ALDOM F.U.H.
ul. Łanowa 63
30-725 Kraków
tel. (12) 411 88 88
faks (12) 294 18 88
e-mail: handel@aldom.pl
www.aldom.pl

ALPOL Sp. z o.o.
ul. H. Krahelskiej 7
40-285 Katowice
tel. (32) 790 76 56
faks (32) 790 76 61
e-mail : alpol@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

Al. Solidarności 15b, 25-211 **Kielce**
tel. (32) 720 39 81
faks (32) 790 76 94
e-mail: kielce@e-alpol.com.pl

ul. Pachońskiego 2a, 31-223 **Kraków**
tel. (32) 790 76 51
faks (32) 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Ochotnicza 10, 20-012 **Lublin**
tel. (32) 790 76 50
faks (32) 790 76 74
e-mail: lublin@e-alpol.com.pl

ul. Wigury 21, 90-319 **Łódź**
tel. (32) 790 76 25
faks (32) 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. Os. Na Murawie 10/2, 61-655 **Poznań**
tel. (32) 790 76 37
faks (32) 790 76 70
e-mail: poznan@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. Modzelewskiego 35/U9
02-679 **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. Stargardzka 7-9, 54-156 **Wrocław**
tel. (32) 790 76 27
faks (32) 790 76 67
e-mail: wroclaw@e-alpol.com.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

AMBIENT SYSTEM Sp. z o.o.
ul. Sucha 25
80-531 Gdańsk
tel. (58) 345 51 95
faks (58) 344 45 95
e-mail: sekretariat@ambientsystem.pl
www.ambientsystem.pl

ANB Sp. z o.o.
ul. Ostrobramska 91
04-118 Warszawa
tel. (22) 612 16 16
faks (22) 612 29 30
e-mail: anb@anb.com.pl
www.anb.com.pl

Zakład Produkcyjno-Usługowo-Handlowy
ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel./faks (71) 363 17 53
e-mail: anma@anma-pl.eu
www.anma-pl.eu

ATLine Spółka Jawna
Krzysztof Cichulski, Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. (42) 657 30 80
faks (42) 655 20 99
e-mail: info@atline.com.pl
www.atline.com.pl

AVISmedia
ul. Żeromskiego 10
64-200 Wolsztyn
tel. (68) 347 09 25
faks (68) 347 09 26
e-mail: office@merlaud.com.pl
www.merlaud.com.pl

Zakłady Kablowe BITNER
ul. Friedleina 3/3
30-009 Kraków
tel. (12) 389 40 24
faks (12) 380 17 00
e-mail: bitner@bitner.com.pl
www.bitner.com.pl

ROBERT BOSCH Sp. z o.o.
ul. Poleczki 3
02-822 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.com.pl

P.W.H. BRABORK Laboratorium Sp. z o.o.
ul. Postępu 2
02-676 Warszawa
tel. (22) 257 68 12
faks (22) 257 68 95
e-mail: brabork@braborklab.pl
www.braborklab.pl

---

bt electronics Sp. z o.o.
ul. Dukatów 10 b
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.
Tulipan House
ul. Domaniewska 50
02-672 Warszawa
tel. (22) 549 23 30
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrand.pl

C&C PARTNERS TELECOM Sp. z o.o.
ul. 17 Stycznia 119,121
64-100 Leszno
tel. (65) 525 55 55
faks (65) 525 56 66
e-mail: info@ccpartners.pl
www.ccpartners.pl

CAMSAT
ul. Prosta 32
86-050 Solec Kujawski
tel. (52) 387 36 58
faks (52) 387 54 66
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: handlowy@cbcpoland.pl
www.cbcpoland.pl

CCX
ul. Ligocka 103
40-568 Katowice
tel. (32) 609 90 80
faks (32) 609 90 81
e-mail: biuro@ccx.pl
www.ccx.pl
www.zamkielektryczne.pl

Centrum Monitorowania Alarmów
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 0 888
faks (22) 546 0 619
e-mail: warszawa@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. Na Niskich Łąkach 26, 50-422 **Wrocław**
tel. (71) 340 0 209
faks (71) 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Racławicka 82, 60-302 **Poznań**
tel./faks (61) 861 40 51
tel. kom. (0) 601 203 664
e-mail: poznan@cma.com.pl

Al. Niepodległości 659, 81-855 **Sopot**
tel. (58) 345 23 24
tel. kom. (0) 693 694 339
e-mail: sopot@cma.com.pl

CEZIM Jolanta Podrażka
ul. Partyzantów 1
96-500 Sochaczew
tel./faks (46) 863 56 50
e-mail: cezim@cezim.pl
sklep@cezim.pl
www.cezim.pl

COM-LM
ul. Ściegiennego 90
25-116 Kielce
tel. (41) 368 71 90
faks (41) 368 71 12
e-mail: biuro@com-lm.pl
www.com-lm.pl

CONTROL SYSTEM FMN Sp. z o.o.
Al. KEN 96/U15
02-777 Warszawa
tel./faks (22) 855 00 17
e-mail: pk@cs.pl
www.cs.pl

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

D+H POLSKA Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
Biuro SAP: (71) 323 52 47
e-mail: biuro@dhpolska.pl
www.dhpolska.pl

Oddziały:
ul. Hagera 41, 41-800 **Zabrze**
tel. (32) 375 05 70
faks (32) 375 05 71

ul. Płochocińska 19 lok. 44-45, 03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

ul. Kielnieńska 134 A, 80-299 **Gdańsk**
tel. (58) 554 47 46
faks (58) 552 45 24

ul. Narutowicza 59, 90-130 **Łódź**
tel. (42) 678 01 32
faks (42) 678 09 20

Biuro Handlowe:
ul. J. Bema 5A, 73-110 **Stargard Szczeciński**
tel. (91) 561 32 02
faks (91) 561 32 29

DANTOM s.c.
ul. Popiełuszki 6
01-501 Warszawa
tel./faks (22) 869 42 70
e-mail: biuro@dantom.com.pl
www.dantom.com.pl

DAR–ALARM
ul. Nieszawska 3C
03-382 Warszawa
tel. (22) 498 60 62
tel./faks (22) 814 10 30

ul. Polnej Róży 2/4
02-798 **Warszawa**
tel./faks (22) 649 27 97
e-mail: handlowy@darsystem.pl
www.darsystem.pl
www.tvtech.com.pl

DELTA BUSINESS SERVICE
Andrzej Bryl
ul. Ciepła 15/50
50-524 Wrocław
tel./faks (71) 367 06 16
e-mail: bok@delta-security.com.pl
www.delta-security.com.pl

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

DOM Polska Sp. z o.o.
ul. Krótka 7/9
42-200 Częstochowa
tel. (34) 360 53 64
faks (34) 360 53 67
e-mail: dom@dom-polska.pl
www.dom-polska.pl

JABLOTRON Ltd.
Generalny dystrybutor:
DPK System
ul. Piłsudskiego 41
32-020 Wieliczka
tel. (12) 288 23 75
faks (12) 278 48 91
e-mail: biuro@dpksystem.pl
www.dpksystem.pl
www.jablotron.pl

Przedsiębiorstwo Usług Inżynieryjnych
DRAVIS Sp. zo.o.
ul. Bukowa 1
40-108 Katowice
tel. (32) 253 99 10
tel./faks (32) 253 70 85
e-mail: dravisdravis@neostrada.pl
info@dravis.pl
www.dravis.pl

DYSKRET Sp. z o.o.
ul. Mazowiecka 131
30-023 Kraków
tel. (12) 423 31 00
tel. kom. (0) 501 510 175
faks (12) 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 812 05 05
faks (22) 812 62 12
e-mail: office@ebs.pl, j.haschka@ebs.pl
www.ebs.pl

EDP Support Polska Sp. z o.o.
ul. Chłapowskiego 33
02-787 Warszawa
tel. (22) 644 53 90
faks (22) 644 35 66
e-mail: jacek.urbanowicz@edps.com.pl
katarzyna.osiecka@edps.com.pl
www.edps.com.pl

---

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

EL-MONT A. Piotrowski
ul. Wyzwolenia 15
44-200 Rybnik
tel. (32) 42 23 889
faks (32) 42 30 729
e-mail: el-mont@el-mont.com
www.el-mont.com

Przedsiębiorstwo Handlowo-Usługowe
ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel./faks (22) 312 06 00 do 02
e-mail: elproma@elproma.pl
www.elproma.pl

ELTCRAC
Centrum Zabezpieczeń
Systemy Domofonowe
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60/61,
292 48 70
faks (12) 292 48 62, 292 48 65
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl

ELZA ELEKTROSYSTEMY
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 266 46 10
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl

EMU Sp. z o.o.
ul. Twarda 12
80-871 Gdańsk
tel. (58) 344 04 01
faks (58) 344 88 77
e-mail: gdansk@emu.com.pl
www.emu.com.pl

Oddział:
ul. Jana Kazimierza 61, 01-267 **Warszawa**
tel./faks (22) 836 54 05, 837 75 93
tel. kom. 0 602 222 516
e-mail: warszawa@emu.com.pl

EUREKA SOFT & HARDWARE
Rynek 13
62-300 Września
tel. (61) 437 90 15
faks (61) 436 27 14
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

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

ul. Grabiszyńska 66e, 53-504 **Wrocław**
tel. (71) 78 74 741
faks (71) 78 74 742
e-mail: factor.wr@factor.pl

FES Sp. z o.o.
ul. Nałkowskiej 3
80-250 Gdańsk
tel. (58) 340 00 41÷44
faks (58) 340 00 45
e-mail: fes@fes.pl
www.fes.pl

GDE POLSKA
ul. Koniecznego 46
32-040 Świątniki Górne
tel. (12) 256 50 25/35
faks (12) 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

GUNNEBO POLSKA Sp. z o.o.
ul. Piwonicka 4
62-800 Kalisz
tel. (62) 768 55 70
faks (62) 768 55 71
e-mail: polska@gunnebo.com
www.rosengrens.pl
www.gunnebo.pl

GV POLSKA Sp. z o.o.
ul. Kuropatwy 26B
02-892 **Warszawa**
tel. (22) 831 56 81, 636 13 73
faks (22) 831 28 52
tel. kom. (0) 693 029 278
e-mail: warszawa@gv.com.pl

ul. Lwowska 74a
33-300 **Nowy Sącz**
tel. (18) 444 35 38, 444 35 39
faks (18) 444 35 84
tel. kom. (0) 695 583 424
e-mail: biuro@gv.com.pl

ul. Racławicka 60a
53-146 **Wrocław**
tel. (71) 361 66 02
faks (71) 361 66 23
tel. kom. (0) 695 583 292
e-mail: wroclaw@gv.com.pl
www.gvpolska.com.pl

HSA SYSTEMY ALARMOWE
Leopold Rudziński
ul. Langiewicza 1
70-263 Szczecin
tel. (91) 489 41 81
faks (91) 489 41 84
e-mail: biuro@hsa.pl
www.hsa.pl

ICS Polska
ul. Żuławskiego 4/6
02-641 Warszawa
tel. (22) 646 11 38
faks (22) 849 94 83
e-mail: biuro@ics.pl
www.ics.pl

ID ELECTRONICS Sp. z o.o.
ul. Przy Bażantarni 11
02-793 Warszawa
tel. (22) 649 60 95
faks (22) 649 61 00
e-mail: sales@ide.com.pl
www.ide.com.pl

INFO-CAM
Al. Kilińskiego 5
09-402 Płock
tel. (24) 266 97 12
tel./faks (24) 266 97 13
e-mail: handlowy@infocam.com.pl
www.infocam.com.pl

Oddział:
ul. Opolska 29, 61-433 **Poznań**
tel. (61) 832 48 94
tel./faks (61) 832 48 75
e-mail: biuro@infocam.com.pl

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. (12) 411 49 79, 411 57 47
faks (12) 411 94 74
e-mail: insap@insap.pl
www.insap.pl

P.W. IRED
Kazimierzówka 9
21-040 Świdnik
tel. (81) 751 70 80
tel. kom. (0) 605 362 043
faks (81) 751 71 80
e-mail: ired@exe.pl
www.ired.com.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 Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 32 48 900
faks (32) 32 48 901
e-mail: handel@kabe.pl
www.kabe.pl, www.kabe.eu

Systemy Alarmowe
KOLEKTOR Sp. z o.o.
ul. Gen. Hallera 2b/2
80-401 Gdańsk
tel. (58) 341 27 31, 341 47 18
faks (58) 341 44 90
e-mail: info@kolektor.com.pl
www.kolektor.com.pl

KOLEKTOR
K. Mikiciuk, R. Rutkowski Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. (58) 553 67 59
faks (58) 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

KRAK-POŻ Sp. z o.o.
Centrum Ochrony Przeciwpożarowej
i Antywłamaniowej
ul. Ceglarska 15
30-362 Kraków
tel. (12) 266 99 85, 266 52 84, 266 95 08
faks (12) 269 25 79
e-mail: biuro@krakpoz.pl
www.krakpoz.pl

P.P.U.H. LASKOMEX
ul. Dąbrowskiego 249
93-231 Łódź
tel. (42) 671 88 00
faks (42) 671 88 88
e-mail: handel@laskomex.com.pl
www.laskomex.com.pl

MAXBAT Sp. J.
ul. Nadbrzeżna 34A
58-500 Jelenia Góra
tel. (75) 764 83 53
faks (75) 764 81 53
e-mail: info@maxbat.pl
www.maxbat.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, 642 45 35
faks (75) 642 45 25
e-mail: info@micronix.pl
www.micronix.pl

MIWI-URMET Sp. z o.o.
ul. Pojezierska 90a
91-341 Łódź
tel. (42) 616 21 00
faks (42) 616 21 13
e-mail: miwi@miwiurmet.com.pl
www.miwiurmet.com.pl

NOMA 2
Zakład Projektowania i Montażu
Systemów Elektronicznych
ul. Plebiscytowa 36
40-041 Katowice
tel. (32) 359 01 11
faks (32) 359 01 00
e-mail: systemy@noma2.com.pl
www.systemy.noma2.pl

Oddziały:
ul. Ryżowa 42, 02-495 **Warszawa**
tel./faks (22) 863 33 40
e-mail: systemy-wa@noma2.com.pl

ul. Brzozowa 71, 61-429 **Poznań**
tel./faks (61) 830 40 46
e-mail: systemy-pz@noma2.com.pl

NORBAIN POLSKA Sp. z o.o.
ul. Szczecińska 1 FA
72-003 Dobra k. Szczecina
tel. (91) 311 33 49
faks (91) 421 18 05
e-mail: info@norbain.pl
www.norbain.pl

Biuro:
ul. Ostrobramska 101 lok. 202
04-041 Warszawa
tel. (22) 465 65 81
faks (22) 465 65 80
infolinia: 0 801 055 075

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
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. Grunwaldzka 119, 60-313 **Poznań**
tel. (61) 657 93 60
poznan@omc.com.pl

PAG Sp. z o.o.
Bogdanka
21-013 Puchaczów
tel./faks (81) 462 51 36, 462 51 26
e-mail: pag@pag.com.pl
www.pag.com.pl

Oddział:
ul. Zemborzycka 112, 20-445 **Lublin**
tel. (81) 748 02 00 ÷ 09
faks (81) 744 90 62

PANASONIC POLSKA Sp. z o.o.
Al. Krakowska 4/6
02-284 Warszawa
tel. (22) 338 11 77
faks (22) 338 12 00
e-mail: dariusz.labedzki@panasonic.com.pl
www.panasonic.pl

PETROSIN Sp. z o.o.
Rynek Dębnicki 2
30-319 Kraków
tel. (12) 266 87 92
faks (12) 266 99 26
e-mail: office@petrosin.pl
www.petrosin.pl

Oddziały:
ul. Fabryczna 22
32-540 **Trzebinia**
tel./faks (32) 618 02 00, 618 02 02

ul. Chemików 1
32-600 **Oświęcim**
tel. (33) 847 30 83
faks (33) 847 29 52

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
ul. Dzielna 1
00-162 Warszawa
tel. (22) 831 15 35, 831 18 97
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
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
ul. Obornicka 276
60-693 Poznań
tel./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: biuro@pulsarspj.com.pl
www.pulsarspj.com.pl

P.P.H. PULSON
ul. Czerniakowska 18
00-718 Warszawa
tel. (22) 851 12 20
faks (22) 851 12 30
e-mail: biuro@pulson.com.pl
www.pulson.eu

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

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

ROPAM Elektronik s.c.
os. 1000-lecia 6A/1
32-400 Myślenice
tel./faks (12) 272 39 71, (12) 379 34 47
e-mail: biuro@ropam.com.pl
www.ropam.com.pl

SAGITTA Sp. z o.o.
ul. Piekarnicza 18
80-126 Gdańsk
tel./faks (58) 322 38 45
e-mail: sagitta@sagitta.pl
www.sagitta.pl

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

SATIE
ul. Łączyny 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 462 30 87
tel. kom. 0 509 849 791
e-mail: info@acie.pl
www.satie.pl

SAWEL Elektroniczne Systemy Zabezpieczeń
ul. Lwowska 83
35-301 Rzeszów
tel. (17) 857 80 60
faks (17) 857 79 99
e-mail: sawel@sawel.com.pl
www.sawel.com.pl

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Wołoska 9
02-583 Warszawa
tel. (22) 33 00 620 ÷ 623
faks (22) 33 00 624
e-mail: office.warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
ul. Wierzbięcice 1, 61-569 **Poznań**
tel. (61) 833 31 53
faks (61) 833 50 37
e-mail: office.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. 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

S.M.A.
System Monitorowania Alarmów 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

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

SOFTEX DATA S.A.
ul. Poleczki 47
02-822 Warszawa
tel. (22) 331 19 90
faks (22) 331 15 11
e-mail: softex@softex.com.pl
www.softex.com.pl

SOLAR POLSKA Sp. z o.o.
ul. Rokicińska 162
92-412 Łódź
tel. (42) 677 58 00
faks (42) 677 58 01
e-mail: centrala@solar.pl
www.solar.pl www.weblink.solar.pl
www.solar.pl/blueenergy

Oddziały:
ul. Radzikowskiego 35, 31-315 **Kraków**
tel. (12) 638 91 00
faks (12) 638 91 22
e-mail: krakow@solar.pl

ul. Witosa 3, 20-330 **Lublin**
tel. (81) 745 59 00
faks (81) 745 59 05
e-mail: lublin@solar.pl

ul. Smoluchowskiego 7, 60-179 **Poznań**
tel. (61) 863 02 04
faks (61) 863 02 70
e-mail: poznan@solar.pl

ul. Heyki 3, 70-631 **Szczecin**
tel. (91) 485 44 00
faks (91) 485 44 01
e-mail: szczecin@solar.pl

ul. Krakowska 141-155, 50-428 **Wrocław**
tel. (71) 377 19 00
faks (71) 377 19 16
e-mail: wroclaw@solar.pl

ul. Łużycka 3B, 81-537 **Gdynia**
tel. (58) 662 00 00
faks (58) 664 04 00
e-mail: gdynia@solar.pl

ul. Armii Krajowej 1, 58-302 **Wałbrzych**
tel. (74) 880 01 14/17
faks (74) 847 00 69
e-mail: walbrzych@solar.pl

ul. Przemysłowa 4F, 33-100 **Tarnów**
tel. /faks (14) 629 80 20
e-mail: tarnow@solar.pl

ul. Glinki 144 bud. A, 85-861 **Bydgoszcz**
tel. (52) 320 50 88/89
faks (52) 362 01 52
e-mail: bydgoszcz@solar.pl

SONY POLAND Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 24 51
tel. kom. (0) 692 403 272, 600 206 117
faks (22) 520 25 77
e-mail: diana.jesionek@eu.sony.com,
marta.malecka@eu.sony.com
www.sonybiz.net/nvm

SPRINT Sp. z o.o.
ul. Jagiellończyka 26
10-062 Olsztyn
tel. (89) 522 11 00
faks (89) 522 11 25
e-mail: olsztyn@sprint.pl
www.sprint.pl

Oddziały:
ul. Budowlanych 64E
80-298 **Gdańsk**
tel. (58) 340 77 00
faks (58) 340 77 01
e-mail: gdansk@sprint.pl

ul. Przemysłowa 15
85-758 **Bydgoszcz**
tel. (52) 365 01 01
faks (52) 365 01 11
e-mail: bydgoszcz@sprint.pl

ul. Heyki 27c
70-631 **Szczecin**
tel. (91) 485 50 00
faks (91) 485 50 12
e-mail: szczecin@sprint.pl

ul. Canaletta 4
00-099 **Warszawa**
tel. (22) 826 62 77
faks (22) 827 61 21
e-mail: warszawa@sprint.pl

S.P.S. Trading Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. (22) 518 31 50
faks (22) 518 31 70
e-mail: warszawa@spstrading.com.pl
www.spstrading.com.pl

Biura Handlowe:
ul. Polska 60, 60-595 **Poznań**
tel. (61) 852 19 02
faks (61) 825 09 03
e-mail: poznan@spstrading.com.pl

ul. Inowrocławska 39C, 53-649 **Wrocław**
tel. (71) 348 44 64
faks (71) 348 36 35
e-mail: wroclaw@spstrading.com.pl

ul. Inflancka 6, 91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.com.pl

ul. 1 Maja 11/2, 10-117 **Olsztyn**
tel. (89) 527 92 72
faks (89) 527 92 30
e-mail: olsztyn@spstrading.com.pl

STRATUS
ul. Nowy Świat 38
20-419 Lublin
tel./faks (81) 743 87 72
e-mail: stratus@stratus.lublin.pl
www.stratus.lublin.pl

SYSTEM 7
ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
infolinia 0 801 000 307
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.sevenguard.com,
www.system7.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

TAC Sp. z o.o.

Oddziały:
ul. Rzymowskiego 53
02-697 **Warszawa**
tel. (22) 313 24 10
faks (22) 313 24 11
e-mail: tac_pol@tac.com
www.tac.com/pl

ul. Arkońska 6 bud. A2
80-387 **Gdańsk**
tel. (58) 782 00 00
faks (58) 782 00 04

ul. Walońska 3-5
50-413 **Wrocław**
tel. (71) 340 58 00
faks (71) 340 58 02

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

TALCOMP SYSTEMY BEZPIECZEŃSTWA
Konrad Talar
ul. Fałęcka 48
30-441 Kraków
tel. (12) 655 85 85, 425 63 67
faks (12) 425 63 68
e-mail: talcomp@talcomp.pl
www.talcomp.pl

TAYAMA POLSKA Sp. J.
ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, (32) 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

Zakład Rozwoju Technicznej Ochrony Mienia TECHOM Sp. z o.o.
ul. Marszałkowska 60/27
00-545 Warszawa
tel. (22) 625 34 00
faks (22) 625 26 75
e-mail: techom@techom.com
www.techom.com

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

TELCOMP-SERVICE Sp. z o.o.
ul. Annopol 4
03-236 Warszawa
tel. (22) 811 02 59
tel. kom. (0) 662 008 600
e-mail: biuro@telcompservice.pl
www.centrum-ts.pl

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
al. Wyzwolenia 70, 71-510 **Szczecin**
tel./faks: (91) 423 70 55
e-mail: witold.brzozowski@telekomunikacja.pl

ul. Rzeczypospolitej 5, 59-220 **Legnica**
tel. (76) 856 60 71
faks (76) 856 60 71
e-mail: marian.sitko@telekomunikacja.pl

ul. Nasypowa 12, 40-551 **Katowice**
tel. (32) 202 30 50
faks (32) 201 13 17
e-mail: dariusz.gawor@telekomunikacja.pl

ul. Rakowicka 51, 31-510 **Kraków**
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Kosmonautów 82, 20-358 **Lublin**
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbigniew.chodkiewicz@telekomunikacja.pl

TRIKON
32-447 Siepraw 1123
tel. (12) 274 61 27
faks (12) 274 51 51
e-mail: biuro@trikon.com.pl
www.trikon.com.pl

UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. (12) 398 99 00
faks (12) 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

Oddziały:
ul. Ratuszowa 11, 03-450 **Warszawa**
tel. (22) 619 22 04
faks (22) 818 64 67

Os. Polan 33, 61-249 **Poznań**
tel. (61) 872 92 08÷10
faks (61) 872 96 30

W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. (52) 345 45 00
tel./faks (52) 584 01 92
e-mail: lukasz.cellari@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

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
2M Elektronik	-	TAK	TAK	TAK	-
3D	TAK	TAK	-	-	TAK
4 COM	-	TAK	TAK	TAK	TAK
AAT Holding	-	TAK	TAK	-	TAK
ACSS ID Systems	-	-	TAK	-	TAK
ADT Poland	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	-
Alarmnet Sp. J.	-	TAK	TAK	-	TAK
Alarmtech Polska	TAK	TAK	-	-	TAK
Aldom	-	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	-
Alpol Sp. z o.o.	-	-	TAK	-	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
ANB	-	TAK	TAK	TAK	TAK
Anma	-	TAK	-	TAK	TAK
Atline Sp. J.	-	TAK	TAK	-	TAK
AVISmedia	-	TAK	TAK	-	TAK
Bitner Zakłady Kablowe	TAK	-	-	-	-
BOSCH	TAK	-	TAK	-	-
P.W.H. Brabork - Laboratorium	-	TAK	TAK	TAK	-
bt electronics	TAK	TAK	TAK	TAK	TAK
C&C Partners	-	TAK	TAK	-	TAK
CAMSAT	TAK	TAK	TAK	-	-
CBC Poland	TAK	-	TAK	-	TAK
CCX	-	TAK	TAK	TAK	TAK
Cezim	TAK	TAK	TAK	-	TAK
CMA Sp. z o.o.	TAK	TAK	TAK	TAK	-
COM-LM	TAK	TAK	TAK	TAK	-
CONTROL SYSTEM FMN	-	TAK	TAK	TAK	-
D-MAX	-	TAK	TAK	-	TAK
D+H Polska	TAK	TAK	TAK	TAK	TAK
DANTOM	TAK	-	TAK	-	-
DAR-ALARM	-	TAK	TAK	TAK	TAK
Delta Business Service	-	TAK	-	TAK	TAK
DG Elpro	-	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	-	-
DPK System	-	-	TAK	-	TAK
Dravis	-	TAK	-	TAK	-
Dyskret	-	TAK	TAK	TAK	TAK
EBS	TAK	-	TAK	-	-
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compil	TAK	TAK	TAK	-	TAK
El-Mont	-	TAK	-	TAK	-
Elproma	-	TAK	-	TAK	-
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	-	TAK	-	TAK	TAK
Emu	-	-	TAK	-	-
Eureka	-	TAK	-	TAK	-
Factor Polska	-	-	TAK	-	TAK
FES	-	TAK	TAK	TAK	-
GDE Polska	-	-	TAK	-	TAK
Gunnebo	TAK	TAK	TAK	TAK	-
GV Polska	-	-	TAK	-	TAK
HSA	-	-	TAK	-	-
ICS Polska	-	-	TAK	-	TAK
ID Electronics	-	TAK	TAK	TAK	-
Info-Cam	TAK	TAK	TAK	TAK	TAK

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Insap	-	TAK	TAK	TAK	TAK
Ired	TAK	TAK	TAK	TAK	-
Janex International	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	-	TAK	-	TAK	-
Kolektor MR	-	TAK	TAK	TAK	-
Krak-Poż	-	TAK	-	TAK	-
Laskomex	TAK	TAK	TAK	-	TAK
Legrand Polska	TAK	TAK	TAK	-	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	-	-	-	TAK
Micronix	-	TAK	TAK	-	-
Miwi-Urmet	TAK	-	TAK	-	TAK
Noma 2	TAK	TAK	TAK	TAK	-
NORBAIN Polska	TAK	-	TAK	-	TAK
OBIS Sp. J.	-	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	-	-	TAK	-	-
PAG	TAK	TAK	TAK	TAK	-
Panasonic	-	-	TAK	-	TAK
Petrosin	-	TAK	-	TAK	-
Pointel	-	TAK	-	TAK	-
POL-ITAL	-	-	TAK	-	-
Polon-Alfa	TAK	-	-	-	-
ProfiCCTV	-	TAK	TAK	-	TAK
Pulsar	TAK	-	TAK	-	-
PPH Pulson	TAK	TAK	TAK	-	-
Radioton	-	-	TAK	-	-
Ramar	TAK	-	TAK	TAK	TAK
ROPAM Elektronik	TAK	-	TAK	-	-
Sagitta Sp. z o.o.	TAK	-	-	-	-
Satel	TAK	-	-	-	-
SATIE	TAK	-	TAK	TAK	TAK
Sawel	-	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	-	-	-	TAK
Secural	TAK	TAK	TAK	-	TAK
S.M.A.	-	TAK	-	TAK	-
SOFTEX Data	-	-	TAK	-	TAK
Solar	-	-	TAK	-	-
Sony	TAK	-	-	-	-
Sprint Sp. z o.o.	-	TAK	-	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK
STRATUS	-	TAK	TAK	-	TAK
SYSTEM 7	TAK	TAK	TAK	-	TAK
TAC	TAK	TAK	TAK	TAK	TAK
Talcomp	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	-	-	TAK	-	TAK
Tayama	TAK	TAK	TAK	TAK	TAK
Techom	-	-	-	-	TAK
Technokabel	TAK	-	-	-	-
Telcomp-Service	-	-	-	-	TAK
TP TELTECH	-	TAK	TAK	TAK	-
Trikon	TAK	TAK	-	TAK	-
UNICARD S.A.	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	-	-
Vision Polska	-	TAK	TAK	-	TAK

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
2M Elektronik	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
3D	-	TAK	-	-	-	-	-	-	-
4 COM	TAK	TAK	TAK	TAK	-	TAK	TAK	TAK	-
AAT Holding	TAK	TAK	TAK	TAK	-	TAK	TAK	-	-
ACSS ID Systems	systemy identyfikacji								
ADT Poland	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
Alarm System	TAK	TAK	TAK	-	-	-	-	-	-
Alarmnet Sp. J.	TAK	TAK	TAK	-	-	TAK	-	TAK	-
Alarmtech Polska	TAK	-	-	-	-	-	-	-	-
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Alkam System	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
Alpol Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Ambient System	TAK	TAK	TAK	TAK	-	-	-	-	TAK
ANB	TAK	TAK	-	TAK	-	TAK	TAK	-	TAK
Anma	TAK	TAK	TAK	TAK	-	TAK	-	-	-
ATLine Sp. j.	TAK	TAK	TAK	-	TAK	TAK	-	-	-
AVISmedia	-	-	-	TAK	-	-	-	-	TAK
Bitner Zakłady Kablowe	-	TAK	-	TAK	-	-	TAK	-	TAK
BOSCH	TAK	TAK	-	TAK	-	-	TAK	-	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
bt electronics	-	-	TAK	-	-	-	-	TAK	-
C&C Partners	-	TAK	-	-	-	-	TAK	-	-
CAMSAT	-	TAK	-	-	-	-	-	-	-
CBC Poland	-	TAK	-	-	-	-	-	-	-
CCX	-	-	TAK	-	-	-	-	TAK	-
Cezim	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
CMA Sp. z o.o.	TAK	-	-	-	-	-	TAK	-	-
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Control System FMN	TAK	TAK	TAK	TAK	-	TAK	-	TAK	-
D-MAX	-	TAK	-	-	-	-	-	-	-
D+H	-	-	-	TAK	-	TAK	-	-	TAK
DANTOM	TAK	TAK	TAK	TAK	-	-	-	TAK	-
DAR-ALARM	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Delta Business Service	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	-	-	TAK	-	-	-	-	TAK	-
DPK System	TAK	TAK	-	-	-	-	TAK	-	-
Dravis	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Dyskret	TAK	TAK	TAK	TAK	-	TAK	-	TAK	TAK
EBS	TAK	-	TAK	TAK	-	TAK	TAK	-	-
EDP Support Polska	-	TAK	TAK	-	TAK	TAK	-	TAK	-
ela-compil	-	-	-	-	-	TAK	-	-	-
El-Mont	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	-
Factor Polska	TAK	TAK	TAK	TAK	TAK	-	-	-	-
FES	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
GDE Polska	TAK	TAK	TAK	-	-	-	-	TAK	-
Gunnebo	-	-	TAK	-	TAK	-	-	TAK	-
GV Polska	-	TAK	-	-	-	-	TAK	-	-
HSA	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
ICS Polska	TAK	TAK	TAK	-	-	-	-	-	-
ID Electronics	TAK	TAK	TAK	-	TAK	-	-	TAK	-
Info-Cam	TAK	TAK	TAK	-	-	TAK	TAK	-	TAK

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Insap	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
Ired	TAK	TAK	TAK	-	-	TAK	TAK	-	-
Janex International	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Krak-Poż	-	-	-	TAK	-	-	TAK	-	TAK
Laskomex	-	TAK	TAK	-	-	-	-	TAK	-
Legrand Polska	-	-	TAK	-	-	-	-	-	-
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
MicroMade	-	-	TAK	-	-	-	-	-	-
Micronix	TAK	TAK	TAK	TAK	-	-	-	TAK	-
Miwi-Urmet	TAK	TAK	TAK	-	TAK	TAK	TAK	TAK	-
Noma 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
NORBAIN Polska	-	TAK	-	-	-	TAK	-	-	-
OBIS Sp. J.	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	-	-	-	-	TAK	-
PAG	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Panasonic	-	TAK	TAK	-	-	TAK	-	-	-
Petrosin	TAK	TAK	TAK	-	-	-	-	-	-
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
POL-ITAL	-	-	TAK	-	-	-	-	TAK	-
Polon-Alfa	-	-	-	TAK	-	-	-	-	-
ProfiCCTV	TAK	TAK	TAK	TAK	-	-	-	-	-
Pulsar	TAK	TAK	TAK	-	-	-	-	TAK	-
PPH Pulson	TAK	-	-	-	-	TAK	TAK	-	-
Radioton	-	TAK	-	-	-	-	-	-	-
Ramar	TAK	TAK	TAK	-	TAK	-	TAK	-	-
ROPAM Elektronik	TAK	-	TAK	TAK	-	-	TAK	-	-
Sagitta Sp. z o.o.	-	-	-	TAK	-	-	-	-	-
Satel	TAK	-	TAK	-	-	-	TAK	-	-
SATIE	-	-	TAK	-	-	-	-	-	-
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	-	-	-
Schrack Seconet Polska	-	-	-	TAK	-	-	-	-	-
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Softex Data	-	TAK	-	-	-	TAK	TAK	-	-
Solar	TAK	TAK	TAK	TAK	TAK	-	TAK	-	TAK
Sony	-	TAK	-	-	-	-	TAK	-	-
Sprint Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
STRATUS	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
TAC	TAK	TAK	TAK	TAK	-	TAK	TAK	-	-
Talcomp	TAK	TAK	TAK	-	TAK	-	-	-	-
Tap – Systemy Alarmowe	TAK	-	TAK	-	-	-	-	-	-
Tayama	TAK	TAK	TAK	-	-	TAK	-	-	TAK
Techom					szkolenia				
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Telcomp-Service					szkolenia				
TP TELTECH	TAK	TAK	TAK	TAK	TAK	-	TAK	-	-
Trikon	-	-	TAK	-	-	-	-	TAK	-
UNICARD S.A.	-	-	TAK	-	-	TAK	-	TAK	-
W2	TAK	-	-	TAK	-	-	-	-	-
Vision Polska	-	-	-	TAK	-	-	-	-	-

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk
teresa@zabezpieczenia.com.pl
Redaktor merytoryczny
Adam Bułaciński
adam@zabezpieczenia.com.pl
Dział marketingu i reklamy
Ela Końka
ela@zabezpieczenia.com.pl
Redaguje zespół:
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Ireneusz Krysowaty
Paweł Niedziejko
Edward Skiepko
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz
Współpraca zagraniczna
Rafał Niedzielski
rafal@zabezpieczenia.com.pl
Współpraca
Marcin Pyclik
Sławomir Wagner
Andrzej Wójcik
Skład i łamanie
Marek Bladoszewski
Korekta
Paweł Karczmarzyk
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

Artykuł sponsorowany:
indywidualne negocjacje (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

Spis teleadresowy:

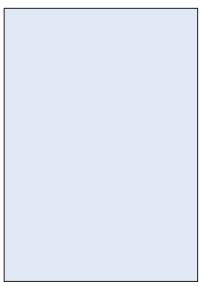
jednorazowy wpis	70 zł

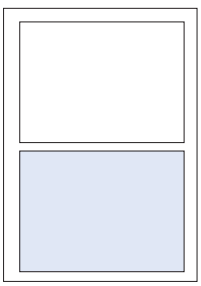
Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji

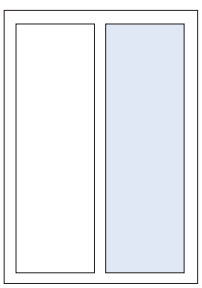
W przypadku zamówienia na 12 emisji 10% rabat

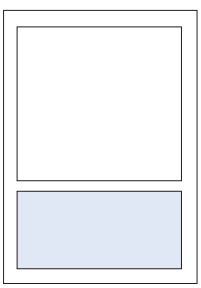
Podane ceny nie uwzględniają podatku VAT (22%)

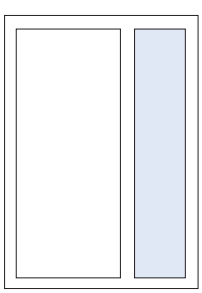
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej **http://www.zabezpieczenia.com.pl** w dziale **Reklama**

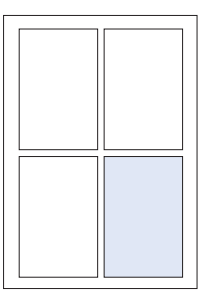

cała strona
(200 x 282 mm + 3mm spad)


1/2 strony
(170 x 125 mm)


1/2 strony
(81,5 x 257 mm)


1/3 strony
(170 x 80,5 mm)


1/3 strony
(53 x 257 mm)


1/4 strony
(81,5 x 125 mm)

Spis reklam

Panasonic
ideas for life

Przetwornik CCD 1,3 Megapiksela, Pozwoli Ci Zobaczyć Więcej

Kamera megapikselowa

Kamera wyposażona w przetwornik CCD 1,3 megapiksela oraz specjalizowany cyfrowy układ przetwarzania sygnału umożliwi Ci obejrzenie każdego szczegółu twarzy, ubrania, a także identyfikację numeru tablicy rejestracyjnej samochodu.

* Porównanie obrazów z kamer konwencjonalnej i megapikselowej i-Pro

Kopułkowa, megapikselowa kamera sieciowa typu dzień/noc
WV-NF302

Megapikselowa kamera sieciowa typu dzień/noc
WV-NP304

Profesjonalny sieciowy system monitoringu wizyjnego dostarcza doskonałej jakości obrazów oraz gwarantuje wysoką jakość całego systemu

Nowe, bardziej zaawansowane kamery serii i-Pro oferują bardzo wysoką jakość obrazu dzięki zastosowaniu przetworników 1,3 megapikseli oraz innych zaawansowanych funkcji, znacznie zwiększając możliwości identyfikacji. Duża pojemność dyskowa rejestratora oraz precyzyjny dekoder pozwalają w pełni korzystać z dobrodziejstw obrazów wysokiej rozdzielczości.

IP

Progresywne wyjście wideo
Funkcja progresywnego skanowania CCD zapewnia, że szybko poruszające się pojazdy, osoby lub inne ruchome przedmioty pozostaną nie rozmyte.

ABS (Adaptive Black Stretch)
Funkcja ABS, wykorzystująca zastrzeżony algorytm przetwarzania obrazu, sprawia, że łatwiej zobaczyć to, co dzieje się w ciemnych częściach obrazu, bez efektu rozmycia jego jasnych części.

Focus Assist
Funkcja Focus Assist ułatwia wybranie optymalnej ostrości obrazu i pozwala w pełni wykorzystać zalety kamer megapikselowych.

Terabajtowa pojemność dyskowa oraz precyzyjny monitoring

Sieciowy rejestrator dyskowy
WJ-ND400

Multikanałowy wideodekoder High Definition
WJ-GXD400

i-Pro Network Surveillance System

i-pro

http://panasonic.net/security/

Panasonic Polska Sp. z o. o.
Al. Krakowska 4/6, 02-284 Warszawa, Polska, Tel.: +48 22 338 11 77 Fax: +48 22 338 12 00; http://panasonic.net/security/

Nasze karty obiegły cały świat.

METODY ZARZĄDZANIA DOSTĘPEM I IDENTYFIKACJĄ

Fizyczna Kontrola Dostępu

Logiczna Kontrola Dostępu

Rozwiązania Wspólne

Dystrybucja Kart

Technologia wklejania dodatkowych elementów

ROZWIĄZANIA TECHNOLOGII INDENTYFIKACJI

Płatność bezgotówkowa

Przemysł i Logistyka

Administracja i Instytucje Rządowe

Żywność i Zwierzęta

hidglobal.com

HID Global, światowy lider technologii kart i czytników kontroli dostępu, przedstawia nowe spektrum bezpiecznej identyfikacji.

Firma HID rozsławiła się dobrą reputacją opartą o najwyższą jakość, pewność technologii i ciągłą innowacyjność w dziedzinie kart i czytników kontroli dostępu. Teraz postanowiliśmy wzbogacić naszą ofertę produkcji kart o nowe możliwości, poczynając od kontroli dostępu poprzez protokoły Ethernet, aż do rozwiązań wykorzystywanych w transporcie publicznym. Wierzymy, iż przyszłość bezpiecznej identyfikacji należy upatrywać w otwartości na nowości, elastycznych produktach i zbieżności technologii. To jest naszym celem, więc jeżeli szukasz nowych rozwiązań identyfikacji zgłoś się do HID. Twoje oczekiwania mogą już być wykorzystane w naszych kartach.

HID

ACCESS choices.