CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 4(74)/2010

ZABEZPIECZENIA

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

W NUMERZE:

ProSYS.freeCom
Integrated Security Systems
www.riscogroup.com

Zintegrowany System Zabezpieczeń

Całkowita integracja...
Najlepszy wybór

RISCO GROUP

Creating Security Solutions. With Care.

riscogroup.com

Risco Group Poland Sp. z o.o.
ul. 17 Stycznia 56, 02-146 Warszawa
tel: +48 22 500 28 40
e-mail: sales-pl@riscogroup.com
www.riscogroup.com

Spis treści

CZASOPISMO ZABEZPIECZENIA 4/2010

Informatyka śledcza, czyli jak ochronić firmę przed nieuczciwymi pracownikami **18**

System bezpieczeństwa obiektu dydaktycznego **36**

Rejestracja obrazu z kamer HD **48**

Zmiany w normie obronnej NO-04-A004 *Obiekty wojskowe. Systemy alarmowe* **76**

Rejestratory cyfrowe firmy Samsung z kompresją H.264

Firma **Samsung** poszerzyła ofertę rejestratorów o **16 nowych modeli z interfejsem sieciowym i z kompresją H.264** . Algorytm kompresji H.264 zapewnia najwyższą jakość obrazu i jednocześnie minimalizuje zapotrzebowanie na przestrzeń dyskową i szerokość pasma.

– *Nasz zespół projektowy skonstruował serię rejestratorów, aby zapewnić rozwiązania do różnych zastosowań, odpowiadające różnym potrzebom* – powiedział **Peter Ainsworth**, Senior Product Manager na Europę działu profesjonalnej techniki zabezpieczeń w Samsung Techwin Europe Limited. – *Istnieją modele oferujące zapis obrazu z rozdzielczością 4-CIF, 2-CIF lub CIF i prędkością 25 kl/s, z wbudowanymi nagrywarkami DVD lub bez nich.*

Wszystkie cyfrowe rejestratory wizyjne posiadają funkcję wirtualnego, progresywnego skanowania (*Virtual Progressive Scan* – VPS), która eliminuje problem nieostrych krawędzi ruchomych obiektów przy zatrzymaniu odtwarzania, a wybrane modele są wyposażone w wyjście HDMI o rozdzielczości 1080p. Oprócz sterowania kamerami przez port RS485 wybrane modele SRD umożliwiają sterowanie poprzez kabel koncentryczny, dzięki czemu nie trzeba stosować dodatkowych kabli do przesyłu danych. Zmniejsza to koszty i skraca czas instalacji.

Dodatkowym ułatwieniem w procesie instalacji i serwisowania jest wielojęzyczny wyświetlacz ekranowy oraz zdejmowalny tylny panel, który umożliwia wymianę lub dodawanie dysków twardych bez potrzeby odłączania kabli. Dane z kas fiskalnych i bankomatów lub z systemu kontroli dostępu można zapisywać w rejestratorze i logicznie powiązać z wybranym kanałem wizyjnym.

Podwójnie realizowany proces kompresji pozwala na utworzenie dwóch strumieni o różnych parametrach: wysokich dla rejestracji oraz niższych dla transmisji sieciowej. Wbudowany serwer sieci WWW umożliwia podgląd na żywo i odtwarzanie zapisanych obrazów, a także wykonanie kopii zapasowej za pośrednictwem przeglądarki internetowej. Cyfrowe rejestratory wizyjne serii SRD są w pełni kompatybilne z opracowanym przez firmę Samsung oprogramowaniem do scentralizowanego zarządzania (*Centralized Management Software* – CMS) SVM-S1, które może integrować wiele systemów zabezpieczeń. Intuicyjne graficzne menu użytkownika (GUI) ułatwia operatorowi na przykład konfigurację każdego kanału przy różnych rozdzielczościach i prędkościach zapisu.

– *W ciągu ostatnich lat cyfrowe rejestratory wizyjne firmy Samsung zasłużyły sobie na znakomitą reputację w branży techniki zabezpieczeń dzięki zapewnieniu wyjątkowej jakości obrazu i doskonałej funkcjonalności. Wierzymy, że ta reputacja zostanie wzmocniona dzięki wprowadzeniu na rynek nowych, zaawansowanych cyfrowych rejestratorów obrazu* – dodał Peter Ainsworth.

Bezpośr. inf. David Solomons
DRS Marketing

Nowe obudowy do kamer firmy Samsung

Samsung wprowadził na rynek nową serię obudów do kamer, wykonanych z odlewanego ciśnieniowo aluminium, zaprojektowanych w oparciu o wskazówki instalatorów i integratorów systemów.

Seria obudów kamer **SHB-4300** ma następujące właściwości ułatwiające montaż:

– boczne otwieranie obudowy umożliwiające instalatorom łatwy i wygodny dostęp podczas pracy;
– trzy dławice umożliwiające oddzielne przeprowadzenie kabli zasilających, wizyjnych i służących do transmisji danych, co chroni przed interferencjami;
– tylne listwy zaciskowe umożliwiające odłączenie zasilania od kamery i od oświetlaczy, co wpływa na bezpieczeństwo pracy instalatora;
– osłona przeciwsłoneczna chroniąca przed bezpośrednim działaniem promieni słonecznych;
– wszystkie trzy obudowy posiadają uchwyt z przepustem kablowym umożliwiający staranne osłonięcie kabla kamerowego i zabezpieczenie go przez aktami wandalizmu; otwory montażowe uchwytu mają gumowe tuleje zabezpieczające, stosowane w przypadku montażu na płaskiej ścianie;
– specjalnie wbudowane u podstawy obudowy oprawy oświetlaczy podczerwieni umożliwiające kierowanie ich promieniowania w tym samym kierunku, w jakim ustawiona jest kamera.

Seria SHB-4300 obejmuje trzy modele obudów. Każdy z nich ma wbudowaną grzałkę i wentylator. Obudowa **SHB-4300H** jest obudową niskonapięciową, zaprojektowaną do zastosowań w zakresie temperatur od -35°C do +50°C. Obudowy **SHB-4300H1** i **SHB-4300H2** mają dodatkową grzałkę umożliwiającą stosowanie kamer w zakresie temperatur od -50°C do +50°C. SHB-4300H1 to obudowa wysokonapięciowa, a SHB-4300H2 – niskonapięciowa.

Bezpośr. inf. David Solomons
DRS Marketing

Kamery termowizyjne Flir w ofercie firmy ATLine

Kamery termowizyjne stają się coraz bardziej popularne w systemach nadzoru wizyjnego. Wielu użytkowników wymaga, aby można było łatwo zintegrować je z nowymi lub już istniejącymi sieciowymi systemami CCTV. Nowe kamery termowizyjne firmy **Flir** są odpowiedzią na te potrzeby.

Firma **ATLine**, która zajmuje się bezpieczeństwem obiektów, wprowadziła do oferty i realizowanych projektów najnowsze modele kamer termowizyjnych Flir.

O kamerach termowizyjnych

Kamery termowizyjne wykorzystują do swojego działania specjalne sensory, które „widzą" energię cieplną wyemitowaną przez obiekt. Energia cieplna lub – inaczej – promieniowanie podczerwone to rodzaj światła, które nie jest widoczne dla ludzkiego oka. Jest to część widma elektromagnetycznego, które odczuwamy jako ciepło (np. emituje je gorący grzejnik). Kamery termowizyjne pozwalają nam zobaczyć to, czego nasze oczy nie widzą. Na podstawie różnicy temperatur pomiędzy obiektami kamery termowizyjne tworzą bardzo wyraźne obrazy. W przeciwieństwie do innych kamer kamery termowizyjne nie potrzebują żadnego źródła światła zewnętrznego, aby wygenerować obraz z dużą ilością szczegółów. Zapewniają one widoczność bez względu na poziom oświetlenia i warunki pogodowe.

Bezpośr. inf. ATLine

PT-Series – zintegrowane kamery termowizyjne i klasyczne z głowicą uchylno-obrotową, kompatybilne z systemami analogowymi i cyfrowymi

Kamery termowizyjne PT-Series pozwalają monitorować obiekty w całkowitej ciemności lub przy niesprzyjającej pogodzie. Precyzja mechanizmu głowicy uchylno-obrotowej zapewnia operatorom dużą dokładność pozycjonowania kamery – zarówno w trybie ręcznym, jak i automatycznym. W przypadku integracji z systemami alarmowymi mechanizm uchylno-obrotowy umożliwia nadzór miejsca wystąpienia alarmu. Kamery PT-Series mogą być łatwo instalowane w sieciach TCP/IP. Możliwe jest także używanie ich w tradycyjnych, analogowych sieciach CCTV.

F-Series – kamery termowizyjne kompatybilne z systemami analogowymi i cyfrowymi

Dzięki zastosowaniu kamer termowizyjnych można zrezygnować z budowy kosztownej infrastruktury oświetleniowej, niezbędnej dla kamer klasycznych. Kamery mogą być łatwo instalowane w sieciach TCP/IP i analogowych systemach CCTV.

D-Series – zewnętrzne kopułkowe kamery termowizyjne kompatybilne z systemami analogowymi i cyfrowymi

Kamery termowizyjne D-Series pozwalają monitorować obiekty w całkowitej ciemności lub przy niesprzyjającej pogodzie. Precyzja mechanizmu głowicy uchylno-obrotowej zapewnia operatorom dużą dokładność pozycjonowania kamery – zarówno w trybie ręcznym, jak i automatycznym. W przypadku integracji z systemami alarmowymi mechanizm uchylno-obrotowy umożliwia nadzór miejsca wystąpienia alarmu. Systemy D-Series są systemami sieciowymi, wyposażonymi w kamerę termowizyjną z przetwornikami o rozdzielczości 320×240 oraz kolorową kamerę CCD dzień/noc z 36-krotnym zoomem optycznym.

Bosch oferuje kamery AutoDome Easy II H.264 IP

Kompaktowa kamera kopułkowa PTZ wytwarza obraz o wysokiej rozdzielczości

Firma **Bosch Security Systems** poszerzyła serię **AutoDome Easy** o wandaloodporną kamerę IP z funkcjami panoramowania, pochylania i zbliżania (*pan/tilt/zoom*), przeznaczoną do zastosowań wewnętrznych i zewnętrznych. Ta wyjątkowa kamera IP została opracowana z myślą o połączeniu funkcjonalności stałopozycyjnych minikamer kopułkowych i tradycyjnych kamer PTZ, wskutek czego oferuje użytkownikom zaawansowane funkcje, jakich nie spotyka się w innych kompaktowych kamerach kopułkowych PTZ.

Kamera AutoDome Easy II IP jest ponad dwa razy mniejsza od tradycyjnej kamery PTZ. Idealnie nadaje się do dyskretnego nadzoru dużych sklepów detalicznych, banków, szkół i budynków biurowych. Jedno urządzenie AutoDome Easy II IP zapewnia takie samo pokrycie jak cztery miniaturowe, stałopozycyjne kamery kopułkowe i kosztuje o połowę mniej niż typowe szybkie kamery kopułowe. Dzięki temu użytkownicy mogą monitorować większy obszar, wykorzystując mniejszą liczbę kamer, oraz obniżyć koszty instalacji i konserwacji systemu.

Aby zmniejszyć obciążenie sieci i koszty pamięci masowej, w nowej kamerze zastosowano kompresję H.264, która zapewnia jakość DVD przy zmniejszonym zapotrzebowaniu na pasmo sieciowe. Kamera AutoDome Easy II IP może generować równocześnie dwa niezależne strumienie danych z kompresją H.264 i o rozdzielczości do 4CIF oraz jeden strumień danych z kompresją M-JPEG. Te trzy strumienie umożliwiają tworzenie obrazów o wysokiej jakości, przeznaczonych do oglądania na żywo, a także obrazów z kompresją M-JPEG, wysyłanych do zdalnego serwera lub innego urządzenia. Wbudowany interfejs iSCSI umożliwia wysyłanie strumienia wizyjnego bezpośrednio do pamięci sieciowej – macierzy iSCSI RAID – w celu rejestracji.

Kamera AutoDome Easy II IP umożliwia również szybki, ciągły obrót o pełne 360 stopni oraz pochylanie i zbliżanie ze zmienną szybkością. 120-krotny zoom (10x optyczny i 12x cyfrowy) z automatycznym ustawianiem ostrości daje użytkownikom możliwość obserwowania obiektów znajdujących się w znacznej odległości. Ponadto kamera jest wyposażona w najnowszą technologię cyfrowego przetwarzania obrazu, zwiększającą jego ostrość, co umożliwia wychwycenie wszystkich istotnych szczegółów obserwowanej sceny. Dzięki znakomitej czułości (poniżej jednego luksa) kamera AutoDome Easy II IP gwarantuje wyraźny kolorowy obraz, nawet przy słabym oświetleniu.

Opcjonalna funkcja inteligentnej analizy obrazu (*Intelligent Video Analysis* – IVA) umożliwia przetwarzanie danych przez kamerę i automatyczne ostrzeganie operatora w przypadku zagrożenia. Dzięki funkcji IVA kamera AutoDome Easy II IP może samodzielnie wykrywać podejrzane zachowania, takie jak bezcelowe wałęsanie się osób, pozostawienie lub zniknięcie jakiegoś przedmiotu czy przekraczanie wirtualnej linii. Ta inteligentna funkcja umożliwia klientom przesyłanie poprzez sieć IP tylko tych obrazów, które są związane z alarmami generowanymi przez IVA, co zmniejsza wymaganą przepustowość sieci i skraca czas reakcji operatora.

Kamera AutoDome Easy II IP jest łatwa w instalacji i obsłudze. Zmiennoogniskowy obiektyw ze sterowaniem proporcjonalnym i automatyczne ustawianie ostrości zapewniają optymalne warunki sterowania kamerą i obserwacji obrazów przy wszystkich stopniach zbliżenia. Dziewięćdziesiąt dziewięć ustawianych pozycji umożliwia użytkownikom obserwację wybranych obszarów monitorowania za naciśnięciem przycisku. Ponadto zgodność ze specyfikacją Open Network Video Interface Forum (ONVIF) gwarantuje kompatybilność z innymi sieciowymi urządzeniami wizyjnymi dowolnego producenta.

Opcje montażu na suficie, na ścianie, w zagłębieniu lub na rurze oraz zestaw do montażu na zewnątrz umożliwiają zainstalowanie kamery niemal wszędzie. Wytrzymała, odporna na ingerencję z zewnątrz, aluminiowa obudowa i solidna kopułka z poliwęglanu chronią kamerę, zapewniając jej wieloletnie, niezawodne działanie nawet w trudnych warunkach.

Bezpośr. inf. Bosch Security Systems

Nowa kamera SCB-3001 w ofercie firmy Samsung

Kamera **SCB-3001** typu dzień/noc z mechanicznym filtrem podczerwieni posiada **procesor DSP SV-V marki Samsung**, który, dzięki nowemu przetwornikowi CCD 960H SuperHAD, umożliwia tworzenie kolorowych obrazów o wysokiej rozdzielczości równej 650 TVL.

Zastosowany w kamerze SCB-3001 procesor DSP SV-V ma także wiele innych właściwości, dzięki którym uzyskiwana jest możliwie najwyższa jakość obrazu, niezależnie od panujących warunków oświetleniowych. Przykładowo – progresywne skanowanie obrazu (VPS), w odróżnieniu od skanowania z przeplotem, zapewnia ostrość konturów poruszających się obiektów lub podczas zatrzymania odtwarzania. Dlatego VPS umożliwia lepszą identyfikację szybko poruszających się osób lub odczytanie tablicy rejestracyjnej jadącego samochodu.

Zaimplementowana w kamerze SCB-3001 funkcja szerokiego zakresu dynamiki obrazu (*Wide Dynamic Range* – WDR) jest rozwiązaniem przeznaczonym do wykorzystania w trudnych warunkach oświetleniowych, takich jak silne tylne oświetlenie lub różne poziomy oświetlenia sceny. Funkcja ta zapewnia prawidłową ekspozycję całego obrazu. Z kolei trzecia generacja systemu redukcji szumów (*Samsung Super Noise Reduction III* – SSNRIII) eliminuje szumy obrazu przy słabym poziomie oświetlenia. Umożliwia to generowanie kolorowych obrazów o wysokiej jakości nawet w warunkach niedostatecznego oświetlenia. Eliminacja szumów pozwala oszczędzić do 70% pamięci rejestratora oraz obniżyć wymaganą szerokość pasma podczas przesyłania obrazów w sieci.

Najbardziej interesującą funkcją analogowej kamery SCB-3001 jest inteligentna analiza obrazu (*Intelligent Video Analysis* – IVA). Kamera posiada m.in. funkcję *optical tripwire*, funkcję detekcji kierunku przemieszczania się obiektu oraz funkcję detekcji znikania i pojawiania się obiektu w zdefiniowanym uprzednio obszarze. Funkcja IVA obejmuje także możliwość reakcji (aktywacji alarmu) na akty wandalizmu, takie jak spryskanie obiektywu kamery farbą lub nieuprawnione przemieszczenie kamery poza jej zwykły obszar obserwacji.

Kamera SCB-3001 ma także możliwość maskowania stref prywatności za pomocą dwunastokątnych obszarów oraz funkcję stabilizacji obrazu (*Digital Image Stabilization* – DIS), która może kompensować pewien zakres drgań kamery spowodowanych wiatrem lub drganiami budynku. Poprzez kabel koncentryczny mogą być przesyłane zarówno dane telemetryczne, jak i sygnał wizyjny, co umożliwia pełny dostęp do funkcji kamery przez cyfrowy rejestrator obrazu kompatybilny z kamerą.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Nowe kamery termowizyjne marki Samsung

Firma **Samsung** wprowadziła dwie nowe kamery termowizyjne do swojej oferty profesjonalnych urządzeń bezpieczeństwa.

Kamery **SCB-9050** o zasięgu detekcji 360 m i **SCB-9051** o zasięgu 1260 m oferują służbom ochrony dodatkowe możliwości wykrywania zagrożeń w przemyśle i systemach bezpieczeństwa obejmujących m.in. ochronę perymetryczną, wykrywanie źródeł strat ciepła czy monitorowanie poziomu cieczy w zbiornikach. Kamery termowizyjne reagują na źródła ciepła, dlatego są w stanie wykrywać przedmioty i osoby w warunkach, w jakich tradycyjne kamery przemysłowe nie mogłyby tego uczynić, np. w warunkach silnego zadymienia, podczas śnieżycy, silnych opadów deszczu czy w gęstej mgle. Dzięki temu są bardzo użyteczne – zarówno w dzień, jak i w nocy – i nie trzeba stosować oświetlenia światłem widzialnym lub promieniami podczerwonymi.

Obie kamery umożliwiają operatorowi wybór trybu generowania obrazu – *white hot*, *black hot* lub *colour scale* – i wyświetlanie na ekranie diagramu zakresu temperatur z automatycznym skalowaniem od najzimniejszej do najcieplejszej części obrazu.

– Takie kamery termowizyjne jak SCB-9050 i SCB-9051 wykrywają różnice w emisji energii promieniowania podczerwonego między obiektami a ich tłem. Ta emisja jest niewidoczna zarówno dla ludzkiego oka, jak i dla konwencjonalnych kamer CCTV

– powiedział **Peter Ainsworth**, Senior Product Manager na Europę firmy Samsung Techwin Europe Limited. – Kamery SCB-9050 i SCB-9051 nie potrzebują żadnego oświetlenia do wygenerowania obrazu, a do wygenerowania wyraźnego obrazu wystarczy im różnica temperatur wynosząca zaledwie 0,08°C.

Kamery SCB-9050 i SCB-9051 o wadze zaledwie dwóch kilogramów (łącznie) i ze zintegrowaną obudową o klasie szczelności IP66 są na tyle lekkie, że można je instalować w większości lokalizacji. Wbudowane menu ekranowe OSD (*on-screen display*) umożliwia łatwą konfigurację parametrów, takich jak kontrast, jasność i ostrość obrazu.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Kopułki A1 już dostępne

Firma **SPS Trading** rozszerzyła linię kamer **APER** wykorzystujących procesory cyfrowej obróbki sygnału A1 (*All in One*). Do wprowadzonych w lutym modeli kompaktowych dołączyły kamery w obudowach kopułkowych. Kamera kopułkowa **VADN-1835H312** z czaszą wykonaną z tworzywa sztucznego jest przeznaczona do zastosowań wewnątrz obiektów, natomiast **VDVR-1835H312** to kamera wandaloodporna o klasie szczelności IP67. Oba modele wyposażono w mechanicznie przesuwany filtr podczerwieni oraz obiektyw o zmiennej ogniskowej 2,8–12 mm.

Kamery A1 charakteryzują się wysoką rozdzielczością 560 TVL (w trybie kolorowym) oraz bardzo wysoką czułością (przy standardowej ekspozycji 1/50 s generują obraz o takiej samej jasności, jak starsze modele w trybie wydłużonej migawki – Sense Up). Sprawia to, że sprawdzają się w monitoringu miejsc słabo oświetlonych, w których obiekty poruszają się szybko.

Ponadto kamery wyposażono w zaawansowany system cyfrowej stabilizacji obrazu, funkcję cyfrowej redukcji szumów, funkcję kompensacji jasnego tła (BLC) z możliwością konfiguracji stref oraz funkcję detekcji ruchu.

Nowe modele kamer mają ulepszone strefy prywatności, które można definiować w formie dowolnego czworoboku, oraz dodatkowe funkcje: cyfrowy zoom, obraz w obrazie, odbicie lustrzane i obraz negatywowy.

Obie kamery posiadają dualny system zasilania niskonapięciowego 12 V_{DC} / 24 V_{AC}.

Bezpośr. inf. Rafał Zieliński
SPS Trading

OSM.2007 Odbiornik systemu monitoringu z innowacyjną funkcją redundancji

Odbiornik Systemu Monitoringu OSM.2007 to urządzenie będące interfejsem pomiędzy urządzeniami służącymi do transmisji danych, zainstalowanymi w dozorowanych obiektach, a oprogramowaniem stacji monitorowania. Włączenie tego elementu w system monitoringu pozwala na tworzenie rozległych systemów telemetrycznych.

Odbiorniki OSM.2007 są wyposażone w szereg funkcji mających na celu podniesienie zarówno komfortu użytkowania, jak i bezpieczeństwa, niezawodności oraz elastyczności systemu.

Najważniejsze z punktu widzenia bezpieczeństwa i niezawodności całego systemu transmisji danych jest zastosowanie rozwiązań redundantnych, zabezpieczających system odbiorczy na wypadek uszkodzenia jego części. Dzięki unikatowej funkcji pracy w klastrze (w grupie komputerów dublujących nawzajem swoje funkcje) w razie awarii jednej z maszyn następuje automatyczne przejęcie jej funkcji przez inny węzeł grupy. Zapewnia to ciągłość pracy odbiornika OSM.2007 bez stałej kontroli i udziału administratora systemu.

Innowacyjność tego rozwiązania została doceniona przez kapitułę konkursu **„Polski Mistrz Techniki Alarmowej 2010”**, a produkowany przez **EBS** odbiornik OSM.2007 wraz z nadajnikiem **PX200N** uzyskał pierwszą nagrodę w kategorii „urządzenia i systemy transmisji alarmu oraz monitoringu”.

Bezpośr. inf. Manuela Małek
EBS

Serwisowy monitor LED

Firma **SPS Trading** wprowadza do oferty nowy poręczny monitor serwisowy typu **LPS-535** o przekątnej 5", w którym wprowadzono kilka nowoczesnych rozwiązań wyróżniających go na tle innych tego typu produktów dostępnych na rynku. Montaż elementów elektronicznych urządzenia jest w całości wykonywany na linii SMT, co oznacza w pełni zautomatyzowany proces produkcji i kontroli jakości. W monitorze nie ma elementów ręcznie przewlekanych i lutowanych.

Wysokiej rozdzielczości panel LCD (640×480) jest podświetlany za pomocą diod LED, a nie, jak wcześniej, za pomocą lamp jarzeniowych. Jest to najważniejsza zaleta tego monitora. Dzięki niej obraz jest dużo bardziej czytelny, nawet w świetle słonecznym, a kąty widzenia są znacznie szersze.

Oprócz konfiguracji ustawień w menu ekranowym podczas regulacji kamer możliwe jest precyzyjne ustawianie ostrości, co z pewnością ułatwi pracę wielu instalatorom. Dzięki podświetleniu diodami LED znacznie wydłuża się także czas pracy urządzenia w przypadku zasilania akumulatorem. Urządzenie może współdziałać ze standardowymi akumulatorami żelowymi, popularnymi w systemach alarmowych, np. EP12-1,2 czy BP12-1,2 – ciągły czas pracy monitora wynosi około czterech godzin. Pracę stacjonarną wspomaga demontowana stopka i zasilacz sieciowy, natomiast działanie w terenie ułatwia wygodny pokrowiec umożliwiający przysłonięcie ekranu – pokrowiec chroni ekran przed bezpośrednim działaniem promieni słonecznych.

Bezpośr. inf. Rafał Zieliński
SPS Trading

Lumin8 – nowy sygnalizator w ofercie RISCO

Z przyjemnością informujemy o rozszerzeniu oferty **RISCO Group** o profesjonalny sygnalizator zewnętrzny **Lumin8** z funkcją podświetlenia logo. Lumin8 jest wyposażony w źródło światła podświetlające logo na przedniej części sygnalizatora, dlatego zapewnia bezpłatną reklamę nawet w całkowitej ciemności.

Lumin8 może być podłączony w klasyczny sposób do dowolnej centrali alarmowej lub pracować na magistrali RISCO Bus w systemach z centralami serii ProSYS. Podłączenie sygnalizatora na magistrali pozwala na zdalne diagnozowanie i konfigurowanie go, co ogranicza koszty i czas serwisowania. Dzięki zdalnej diagnostyce instalator odczytuje parametry pracy Lumin8, takie jak napięcie i prąd akumulatora, napięcie zasilania oraz pobór prądu części optycznej i akustycznej.

Lampa stroboskopowa, wykonana w zgłoszonej do opatentowania technologii SLT, charakteryzuje się bardzo długim czasem żywotności sięgającym nawet 50000 godzin. Źródłem światła są montowane powierzchniowo diody LED, które gwarantują bardzo wysoką niezawodność. Dwa piezoelektryczne sygnalizatory dźwiękowe zapewniają głośność na poziomie 114dBA/1m. Odporna na zniszczenie poliwęglanowa obudowa jest zabezpieczona przed oddziaływaniem promieniowania UV. Konstrukcja wewnętrznej obudowy płytki elektronicznej zapewnia pyłoszczelność i wodoszczelność w klasie szczelności IP65.

Symbol handlowy produktu to RS401200000A. W celu uzyskania dodatkowych informacji prosimy o kontakt z lokalnym przedstawicielem handlowym RISCO Group lub odwiedzenie strony www.riscogroup.com.

Bezpośr. inf. Norbert Góra
RISCO Group Poland

Wzmocnienie pozycji RISCO Group po akwizycji Electronics Line 3000

RISCO Group, wiodący dostawca zintegrowanych rozwiązań z zakresu bezpieczeństwa, wzmocniła swoją pozycję na rynku elektronicznych systemów zabezpieczeń po przejęciu pakietu kontrolnego w firmie **Electronics Line 3000 Ltd**, która jest dostawcą systemów bezpieczeństwa dla rynku rezydencjalnego oraz małych i średnich obiektów komercyjnych.

Celem RISCO jest utrzymanie niezależnego działania firmy Electronics Line i portfela jej produktów. Rozszerzenie oferty firmy o rozwiązania wideo i systemy zarządzania, przy ścisłej współpracy z jej głównymi partnerami na świecie, ma uczynić z Electronics Line lidera grupy RISCO na rynku produktów dla domów i mieszkań.

– *Przejęcie Electronics Line umacnia pozycję i ofertę RISCO na rynku domów i mieszkań. Ten rozwijający się segment sprzedaży wymaga stosowania najwyższej jakości rozwiązań technologicznych w konkurencyjnych cenowo i łatwych w obsłudze systemach* – powiedział **Moshe Alkelai** (na zdjęciu w środku), prezes i dyrektor generalny RISCO Group.

Electronics Line 3000 Ltd jest wiodącym światowym dostawcą zdalnie zarządzanych, bezprzewodowych systemów bezpieczeństwa przeznaczonych do powszechnego stosowania. Integruje różne technologie i rozwiązania w celu dostarczania produktów umożliwiających dwukierunkowe przesyłanie danych, dźwięku i wideo w czasie rzeczywistym. Firma tworzy unikalne rozwiązania dla alarmowych centrów odbiorczych, dystrybutorów systemów zabezpieczeń i firm zajmujących się zarządzaniem nieruchomościami. Electronics Line 3000 to spółka notowana na giełdzie we Frankfurcie (XETRA: ELN).

Bezpośr. inf. Norbert Góra
RISCO Group Poland

Nowa klawiatura dotykowa w ofercie RISCO

Oferta produktów **RISCO Group** wzbogaciła się o klawiaturę dotykową w kolorze białym. Ta elegancka, unikatowa w swojej stylistyce i wspaniale komponująca się z nowoczesnymi wnętrzami klawiatura jest przeznaczona do stosowania w systemach sygnalizacji włamania i napadu RISCO serii **ProSYS**.

Panel, który jest wyposażony w ekran dotykowy o przekątnej 7 cali, zaspokoi potrzeby wymagających użytkowników. Wyświetlane menu umożliwia łatwy dostęp do różnych funkcji systemu alarmowego ProSYS. Dostępny jest także model klawiatury z wbudowanym czytnikiem zbliżeniowym 13,56 MHz, który umożliwia włączanie i wyłączanie systemu alarmowego za pomocą identyfikatora zbliżeniowego w formie breloka.

Wbudowany interfejs do podłączenia komputera z oprogramowaniem Upload/Download ułatwia instalatorowi programowanie i diagnostykę systemu. Głośność brzęczyka oraz jasność i kontrast wyświetlacza są regulowane. Klawiatura dotykowa RISCO jest stosowana w nowoczesnych biurach oraz obiektach rezydencjalnych i apartamentowych.

Klawiatura w kolorze białym będzie dostępna na rynku polskim w III kwartale 2010 r. Symbole handlowe produktu to RP128KP0200A i RP128KPP200A (wersja z czytnikiem zbliżeniowym). Aktualnie jest już w sprzedaży klawiatura w kolorze czarnym o identycznych parametrach. W celu uzyskania dodatkowych informacji prosimy o kontakt z lokalnym dystrybutorem produktów RISCO Group.

Bezpośr. inf. Norbert Góra
RISCO Group Poland

Ujawniono nominowanych do nagród

Detektor International 2010

Kierownictwo redakcji magazynu ***Detektor International*** potwierdziło kandydatów do nagród **Detektor International 2010** po starannej ocenie nowych, innowacyjnych wyrobów, które zostały wprowadzone na rynek sprzętu *security* w ciągu ostatnich 12 miesięcy. Nagroda Detektor International to jedyna nagroda przemysłowa, do której kandydaci nie są nominowani przez dostawców rynku *security*, tylko przez redakcję magazynu. Ten fakt spowodował, że zdobyła renomę. W tym roku nominowano następujące wyroby i producentów:

1) W kategorii kontroli dostępu:
- **Aperio E100DS** – bezprzewodowy czytnik drzwiowy firmy **Assa**;
- **Omnikey 2061** – czytnik z łączem bluetooth firmy **HID**;
- **iLoq Privos** – system zamknięć dla domów i niewielkich obiektów komercyjnych stworzony przez firmę **Ilon**;
- **D-station** – system kontroli dostępu firmy **Suprema** odblokowujący przejście na podstawie analizy odcisku palca i po rozpoznaniu twarzy.

2) W kategorii alarmowych systemów detekcji włamania:
- **DALM 5000** – dialer alarmowy firmy **Dualtech** stworzony w technologii IP, stosowany jako dialer zewnętrzny;
- **CommPact** – mały, bezprzewodowy system sterująco-alarmowy firmy **Electronics Line 3000** przeznaczony do zastosowania w domach i niewielkich obiektach komercyjnych;
- **Radar** – system ochrony obwodowej firmy **GPS Standard**, który wykorzystuje fale elektromagnetyczne;
- **AIM100** – infradźwiękowy, antywłamaniowy detektor akustyczny firmy **iDTEQ**.

3) W kategorii CCTV:
- **AV8365 8 Megapixel 360° Panoramic** – sieciowa, megapikselowa kamera panoramiczna (360°) firmy **Arecont Vision**;
- **Control Center 4.6** – oprogramowanie firmy **Avigilon** przeznaczone do urządzeń HD, stworzone do zarządzania otwartą siecią wizyjną;
- **Q1910-E** – termiczna kamera sieciowa firmy **Axis Communications**;
- **Coldstore** – cyfrowy system pamięci obserwacyjnej stworzony przez firmę **Veracity**.

Kryteria nominacji do nagrody obejmują nie tylko rozwiązania techniczne, ale i opakowanie oraz ogólną prezentację wyrobu, która może być również podstawą do oceny obsługi.

Finał i rozdanie nagród nastąpi 15 września 2010 r. podczas wystawy Skydd w Sztokholmie.

Bezpośr. inf. www.securityworldhotel.com
Opracowanie: Redakcja

Nowy moduł kontrolera w ofercie firmy roger®

Firma **Roger**, krajowy lider w dziedzinie profesjonalnych **systemów kontroli dostępu**, wzbogaca swą ofertę o **nowy moduł kontrolera PR411DR**. Urządzenie jest kontrolerem pojedynczego przejścia i stanowi uzupełnienie znanej serii standardowych kontrolerów dostępu PRxx1.

PR411DR może pracować jako autonomiczny punkt kontroli dostępu lub jako element sieciowego systemu RACS. Urządzenie jest przystosowane do pracy z jednym lub dwoma zewnętrznymi czytnikami dostępu. Mogą to być zarówno czytniki popularnej serii PRT produkowanej przez Roger, jak również dowolne inne czytniki wyposażone w interfejs Wiegand. Możliwość współpracy z czytnikami Wieganda jest szczególnie wskazana w sytuacji, gdy w danym obiekcie są już zainstalowane tego typu czytniki lub gdy zachodzi potrzeba dołączenia do kontrolera czytników specjalnych, takich jak czytniki dalekiego zasięgu, czytniki biometryczne itp.

Cechą odróżniającą PR411DR od innych kontrolerów dostępnych na rynku jest obudowa przystosowana do montażu na standardowej szynie DIN. Takie rozwiązanie zdecydowanie upraszcza proces montażu kontrolera, a dodatkowo umożliwia wykorzystanie różnych obudów przeznaczonych do sprzętu elektrotechnicznego. Daje to także możliwość podłączenia kontrolera w istniejącej już obudowie zawierającej urządzenia elektryczne i pozwala zredukować przestrzeń zajmowaną przez instalację KD. W przypadku zlokalizowania kilku kontrolowanych przejść w bliskiej odległości (korytarze, śluzy) można umieścić kilka kontrolerów w jednej obudowie i doprowadzić kable wyłącznie do czytników i elementów wykonawczych typu elektrozaczep lub zwora magnetyczna. W przypadku produktów firmy Roger maksymalna odległość między kontrolerem a czytnikiem wynosi 150 metrów, jest więc wystarczająca w zdecydowanej większości typowych zastosowań.

PR411DR, w odróżnieniu od pozostałych kontrolerów serii PRxx1, umożliwia ręczne ustawianie adresu urządzenia za pomocą miniaturowych zworek. Kontroler posiada wbudowany moduł zasilacza o wydajności prądowej 1,5 A, z możliwością obsługi akumulatora awaryjnego.

Bezpośr. inf. Filip Paprocki
Roger

Odkryj nieznane

Seria SRD rejestratorów marki Samsung z kompresją H.264

Seria SRD zawiera wszystko czego można oczekiwać od rejestratora, dlatego chcielibyśmy skupić Państwa uwagę na funkcjach, których się nie spodziewacie:

- Własna implementacja algorytmu kompresji H.264 opracowana przez firmę Samsung, pozwalająca zaoszczędzić przestrzeń dyskową z jednoczesną poprawą jakości obrazów.
- Wyjście HDMI z możliwością przeskalowania obrazów do rozdzielczości 1080p.
- Usuwalny tylny panel pozwalający na montaż i wymianę twardych dysków bez konieczności rozłączania połączeń kablowych.
- Wbudowana funkcja wirtualnego, progresywnego skanowania (VPS), która eliminuje zjawisko rozmycia krawędzi poruszających się obiektów przy obserwacji zatrzymanych obrazów.

Zaimplementowany serwer WWW pozwala na podgląd na żywo oraz odtwarzanie obrazów, z możliwością kopiowania danych poprzez przeglądarkę internetową. Dodatkowo darmowe oprogramowanie zarządzające (CMS) o nazwie SVM-S1 posiada zaawansowane funkcje sieciowe, tworząc w pełni zintegrowany system.

Ponadto wszystkie 16 modeli z serii SRD posiada ten sam intuicyjny, graficzny interfejs użytkownika (GUI), co czyni konfigurację wyjątkowo łatwą.

Bezpieczeństwo, które przekracza Twoją wyobraźnię!

Seria urządzeń SRD

Numer części	Kompresja	Kanały	Napęd DVD (sufiks "D")	Wewnętrzne magistrale HDD (sufiks "D")	Prędkość zapisu		
SRD-1670(D)	H.264	16	Nie (Tak)	6(5)	4-CIF = 400 (kl./s)		
SRD-1650(D)	H.264	16	Nie (Tak)	6(5)	4-CIF = 100 (kl./s)	2-CIF = 200 (kl./s)	CIF = 400 (kl./s)
SRD-1630(D)	H.264	16	Nie (Tak)	6(5)	4-CIF = 50 (kl./s)	2-CIF = 100 (kl./s)	CIF = 200 (kl./s)
SRD-1610(D)	H.264	16	Nie (Tak)	6(5)	4-CIF = 25 (kl./s)	2-CIF = 50 (kl./s)	CIF = 100 (kl./s)
SRD-870(D)	H.264	8	Nie (Tak)	6(5)	4-CIF = 200 (kl./s)		
SRD-850(D)	H.264	8	Nie (Tak)	6(5)	4-CIF = 50 (kl./s)	2-CIF = 100 (kl./s)	CIF = 200 (kl./s)
SRD-830(D)	H.264	8	Nie (Tak)	6(5)	4-CIF = 25 (kl./s)	2-CIF = 50 (kl./s)	CIF = 100 (kl./s)
SRD-470(D)	H.264	4	Nie (Tak)	2(1)	4-CIF = 100 (kl./s)		

T **+420 222 866 002, +420 602 532 103**
E **STEsecurity@samsung.com**
W **samsungsecurity.com**

Biuro Regionalne:
Samsung Techwin Europe Ltd
Římská 20, 120 00, Praha 2, Czechy

SAMSUNG

Ogólnopolskie Szkolenie Projektowe **Schrack Seconet 2010**

16 czerwca 2010 r. w Szkole Głównej Służby Pożarniczej w Warszawie odbyło się kolejne **Ogólnopolskie Szkolenie Projektowe firmy Schrack Seconet Polska** – jednego z największych i najbardziej znanych producentów systemów ochrony przeciwpożarowej na świecie.

W szkoleniu wzięło udział około **300 osób** (tym samym został pobity kolejny rekord frekwencji), głównie projektantów SSP oraz specjalistów z branży zabezpieczeń. Oprócz przedstawicieli firmy Schrack Seconet Polska w gronie referentów znaleźli się zaproszeni goście: **Jerzy Ciszewski** i **Janusz Sawicki** z Instytutu Techniki Budowlanej oraz **Edward Skiepko**, reprezentujący Szkołę Główną Państwowej Straży Pożarnej. Organizatorzy spotkania umożliwili również prezentację systemów automatyki budynkowej firmie Delta Controls.

Pierwszą część spotkania rozpoczął **prezes zarządu Schrack Seconet Polska – Grzegorz Ćwiek**, który powitał uczestników i wprowadził ich w tematykę szkolenia. Jako pierwszy wystąpił Janusz Sawicki, który wygłosił referat pt. *Podstawy formalno-prawne projektowania systemów przeciwpożarowych*. Edward Skiepko wprowadził uczestników szkolenia w tematykę bezpieczeństwa pożarowego instalacji elektrycznych, wygłaszając referat pt. Instalacje elektryczne funkcjonujące w trakcie pożaru – kryteria doboru oraz zasady wykonywania instalacji z punktu widzenia bezpieczeństwa pożarowego. Następnie **dyrektor techniczny firmy – Krzysztof Kunecki** – zaprezentował nowości w ofercie Schrack Seconet, m.in. najnowszą centralę sygnalizacji pożarowej i sterowania gaszeniem **Integral IP MX**, koncepcję sieci kratowych oraz **Integral LAN** – elastyczne rozwiązanie przeznaczone do zastosowania w najbardziej „wymagających" obiektach.

Po pierwszej części szkolenia uczestnicy zostali zaproszeni na obiad, podczas którego toczono dyskusje dotyczące aktualności prawnych i kwestii związanych z rzetelnym przygotowaniem projektu zaawansowanych systemów zabezpieczeń budynku.

Drugą część spotkania rozpoczął kierownik ds. produktu w Schrack Seconet Polska – **Paweł Tomaszewski**, który zasygnalizował najnowsze rozwiązania z dziedziny komunikacji w obiektach służby zdrowia – system przyzywowy i komunikacji **Visocall IP**. Uczestnicy spotkania zostali zaproszeni na szkolenie z tego zakresu. W tej części spotkania Jerzy Ciszewski poruszył zagadnienia związane z *Nowelizacją rozporządzenia MSWIA w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia*, a także szczegółowo omówił zasady wydawania dopuszczeń do użytkowania wyrobów, których dotyczy ta nowelizacja, uwzględniając najważniejsze zmiany i ich wpływ na zasady projektowania SSP. Ponadto Jerzy Ciszewski przedstawił aktualności z zakresu projektowania systemów sygnalizacji pożarowej – również takich, które mają być zastosowane w magazynach wysokiego składowania.

W drugiej części spotkania zostały omówione praktyczne aspekty stosowania coraz bardziej popularnych, także w Polsce, systemów wczesnej detekcji. W związku z tym Krzysztof Kunecki szczegółowo scharakteryzował system zasysający Schrack Seconet **AirSCREEN ASD 535**, koncentrując się przede wszystkim na jego praktycznym zastosowaniu.

Moderatorem spotkania był Grzegorz Ćwiek. Głównym celem jego wystąpień było uświadomienie uczestnikom szkolenia, jak ogromną wagę ma rzetelne przygotowanie projektu zaawansowanych systemów bezpieczeństwa. Prezes Schrack Seconet Polska wielokrotnie podkreślał bardzo duże zaangażowanie firmy w fazę projektową każdego obiektu i zaoferował pomoc wszystkim obecnym na sali projektantom i specjalistom z branży. Firma przygotowała narzędzia, które są niezbędne w procesie projektowania systemów sygnalizacji pożarowej, wykorzystując najnowszą technologię Schrack Seconet.

Krzysztof Kunecki przypomniał uczestnikom zalety **zdalnego dostępu do systemu Schrack Seconet**, oferowanego w dwóch wariantach: **Integral Remote Control Panel** – dla użytkowników systemu – oraz **Remote Access** – dla firmy serwisowej. Oprogramowanie Remote Access umożliwia m.in. zdalne monitorowanie, obsługę, konfigurację oraz uruchamianie systemu sygnalizacji pożarowej. Praktyczna prezentacja systemu sygnalizacji pożarowej firmy Schrack Seconet udowodniła, że dzięki niemu można znacznie ograniczyć koszty serwisu i konserwacji.

Uczestnicy spotkania mieli okazję zapoznać się nie tylko z aktualnościami dotyczącymi zasad projektowania, przedstawionymi przez gości Schrack Seconet Polska, ale również z nowościami w ofercie firmy. W trakcie wystąpień słuchacze mogli również uzyskać odpowiedzi na pytania związane z najnowszymi wytycznymi i regulacjami prawnymi. W spotkaniu uczestniczył przedstawiciel firmy **Delta Controls**, jednego z partnerów Schrack Seconet, który zaprezentował najnowsze rozwiązania z dziedziny automatyki budynkowej. Szkolenie zakończył prezes firmy, który podziękował za uczestnictwo i zaprosił do dalszej współpracy.

Ogólnopolskie szkolenia Schrack Seconet, które niezmiennie odbywają się o tej porze roku już od prawie 15 lat, są największymi tego typu szkoleniami w branży zabezpieczeń.

Bezpośr. inf. Marta Nowak
Schrack Seconet Polska

SATEL wspiera GOPR

W 2007 roku firma **SATEL** rozpoczęła współpracę z Górskim Ochotniczym Pogotowiem Ratunkowym (GOPR). Dbanie o bezpieczeństwo, życie i mienie ludzkie jest dla firmy SATEL głównym celem działalności, dlatego wspieranie takiej organizacji jak GOPR, która powstała, aby nieść pomoc ludziom, których zdrowie lub życie jest zagrożone, zapobiegać wypadkom w górach oraz chronić środowisko górskie, jest zgodne z przesłaniem jakie towarzyszy firmie SATEL.

8 czerwca 2010 r. w siedzibie firmy SATEL została podpisana umowa, której przedmiotem jest kontynuacja współpracy. Umowę uroczyście podpisali: Jan Łuszczewski – prezes zarządu GOPR, Jacek Dębicki – naczelnik GOPR, Ireneusz Kowaluk i Leszek Polakiewicz – członkowie zarządu firmy SATEL.

Środki finansowe przekazane na ręce Zarządu Głównego GOPR zostaną przeznaczone na szkolenia prawie 300 ratowników GOPR w zakresie udzielania kwalifikowanej pierwszej pomocy medycznej. Celem szkoleń będzie przede wszystkim zdobycie przez ratowników umiejętności praktycznych, które będą mogli wykorzystywać podczas codziennej pracy w górach. Zakres szkoleń przeprowadzanych w Centrum Szkoleń Medycznych GOPR w Zieleńcu jest oparty na wytycznych światowych organizacji ratowniczych, medycznych i specjalistycznych, takich jak np. BLS-AED, BTLS, ILCOR, IKAR-CISA.

Stacje Centralne i Ratunkowe należące do GOPR zostały wyposażone przez firmę SATEL w urządzenia alarmowe. Dzięki temu znacznie zmniejszyła się liczba włamań i kradzieży sprzętu przeznaczonego do ratowania ludzi.

GOPR zatrudnia 105 ratowników etatowych, a wspomaga ich 1346 ratowników ochotników i 222 kandydatów na ratowników. Roczny bilans działalności ratowniczej w 2009 r. to: 2038 interwencji, 3235 akcji i 105 wypraw ratunkowych (w tym 37 z użyciem śmigłowca), 5543 uratowanych osób.

Bezpośr. inf. Agnieszka Nocuń
Satel

Zapraszamy do obejrzenia fotoreportażu (*zabezpieczenia.com.pl*)

Nowe wyzwania dla zarządzania bezpieczeństwem i ochroną obiektów

Artykuł omawia podstawowe zagadnienia przedstawione na konferencji, wskazuje na szereg zmian w postaci i składzie chronionych obiektów. Jest skrótem materiału wprowadzającego do prac I Konferencji Zarządzania Bezpieczeństwem Obiektów, która odbyła się w ramach SECUREX 2010. Autor, będący współprowadzącym obrady, prezentuje sytuację wyjściową dla obrad, skrótowo omawia zrealizowany program obrad oraz odnosi się do pytań zadawanych na sali oraz zebranych uwag kuluarowych

W dniu 26 kwietnia 2010 roku, w ramach wielu spotkań zawodowych składających się na konferencję SECUREX 2010, odbyła się I Konferencja Zarządzania Bezpieczeństwem Obiektów, organizowana pod patronatem Prezesa PKN przez Stowarzyszenie POLALARM we współpracy z Dyrekcją MTP. Prezentacje i obrady konferencji prowadzone były pod ogólnym, wynikającym z bieżącej sytuacji hasłem:

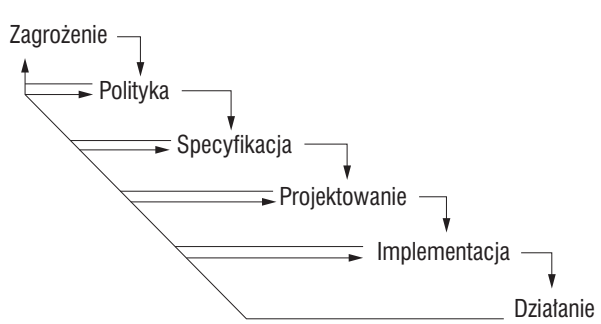
Nie da się poprawnie (efektywnie) zarządzać czymś, czego sami nie znamy dostatecznie, co do jego zmiennej istoty, szerokich granic i ewoluujących potrzeb.

Podstawą merytoryczną konferencji była świadomość jej organizatorów co do konieczności dokonania niezbędnych zmian w podejściu do problematyki ochrony i zapewnienia bezpieczeństwa obiektów poprzez doskonalenie metod zarządzania bezpieczeństwem, a nie wyłącznie dalszą rozbudowę systemów i środków ochrony.

1. Działania na rzecz bezpieczeństwa obiektów

Z zebranych doświadczeń (konsultacje i audyty bezpieczeństwa) wynika jednoznacznie, że tylko nieliczne instytucje (firmy, przedsiębiorstwa, korporacje) prowadzą wyodrębnione działania na rzecz eliminacji lub minimalizacji zagrożeń w zgodzie ze specyfiką swego funkcjonowania, projektując wdrożenia zabezpieczeń adekwatne do przyjętej polityki bezpieczeństwa i możliwie maksymalnie skuteczne na obszarze ich działania.

W większości przypadków spotykamy „architekturę wyspową", kiedy to w firmie funkcjonują odrębne polityki bezpieczeństwa fizycznego, środowiskowego, pożarowego, danych osobowych, informacji, bo o tajemnicach biznesowych, służbowych i finansowo-księgowych na ogół wyłącznie mówi się, a bardzo rzadko precyzyjnie opisuje się je. Takie sytuacje sprzyjają przypadkowemu ujawnianiu chronionej wiedzy poza komórkami organizacyjnymi, których ona bezpośrednio dotyczy. W takich sytuacjach trudno też mówić o kompleksowym rozwiązywaniu pojawiających się problemów i zintegrowanym zarządzaniu bezpieczeństwem połączonym z zachowaniem ciągłości i trwałości funkcjonowania danej firmy. Szereg szczegółowych odniesień do tych zjawisk omówili w swoich wystąpieniach konferencyjnych Maciej Byczkowski – prezes ENSI i zarazem prezes zarządu Stowarzyszenia Administratorów Bezpieczeństwa Informacji – oraz Krzysztof Ciesielski – prezes I-SEC oraz członek zarządu POLALARM-u i rzeczoznawca STZOiMoZB. Fragmentarycznie odnieśli się do tego problemu wszyscy referujący – odpowiednio do swoich głównych tematów wystąpień.



Rys. 1. Łączenie oddziaływań w ochronie

Istota proponowanego spojrzenia na całość problematyki tkwi nie tyle w konieczności wprowadzania zmian w samej ochronie w odniesieniu do obszarów, w których jej stosowanie jest narzucone ustawowo, co w potrzebie zintegrowania już posiadanych doświadczeń w jednym, wspólnym podejściu systemowym do tych wielu współbieżnych procesów.

1.1. Zmiany – rozszerzenie potrzeb ochronnych

Zasada wymagalności bezpieczeństwa jest prosta:

- **różnorodność oddziaływań ochronnych ⇔ różnorodność zagrożeń (niezależnie od rodzaju i charakteru chronionego obiektu)**

Współczesne środowisko stawia przed nami coraz to inne, różne, ale zawsze wysokie wymagania. W celu ich potwierdzenia rozpatrzmy hipotetycznie wymiar możliwych do wystąpienia zagrożeń dla różnych obiektów:

1) obiekt ochrony – lotnisko i jego elementy:
   – terminal, pasażerowie, bagaże,
   – samoloty, obsługa techniczna, paliwa,
   – drogi startu i kołowania, infrastruktura bezpieczeństwa,
   – rozległość zagrożeń (wymiary stref bezpieczeństwa), znaczenie wysokości;
2) obiekt ochrony – port morski i jego elementy:
   – statki i ich ładunek,
   – infrastruktura przeładunkowa,
   – masowość i różnorodność,
   – rozległość zagrożeń (wymiary stref bezpieczeństwa), znaczenie głębokości;

3) obiekt ochrony – obiekt sportowy i jego elementy:
– stadion, widzowie, sportowcy, sprawozdawcy,
– obsługa techniczna, infrastruktura techniczna i użytkowa,
– drogi ewakuacji, infrastruktura bezpieczeństwa,
– rozległość zagrożeń (wymiary stref bezpieczeństwa), znaczenie masowości.

Oczywiście to nie wszystkie ekstremalnie rozległe obiekty – może to być także metro, dworzec kolejowy, duża hala targowa/wystawowa, duża baza logistyczna itp.

1.2. Wiedza czynnikiem bezpieczeństwa

Świadomość zagrożeń obiektów u osób zarządzających ich bezpieczeństwem jest czymś oczywistym, ale jakże często zapomina się o szeregowych pracownikach, o ich przeszkoleniu i uczulaniu ich na symptomy potencjalnych zagrożeń (we wszystkich kategoriach – od szpiegostwa przemysłowego po bezpieczeństwo środowiskowe).

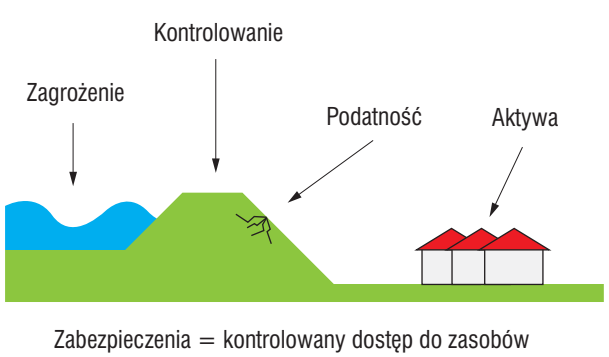
Należy zwrócić uwagę na potrzebę wielowymiarowości działań ochronnych i konieczność zmiany optyki analizy zagrożeń, zanim te zagrożenia – jako zmaterializowane ryzyka – spowodują krach funkcjonowania naszych, dotychczas dobrze prosperujących, firm/instytucji/korporacji.

„Porządek nie jest tam, gdzie mamy wielu sprzątających – jest tam, gdzie nie ma brudzących". Ta myśl przypisywana Konfucjuszowi – wielkiemu chińskiemu filozofowi – w pełni oddaje ideę konieczności zarządzania wiedzą o zagrożeniach i bezpieczeństwie jako podstawy działań ochronnych we współczesnym świecie. Należy udostępniać tę wiedzę w sposób czytelny i ograniczony, a także dostosować ją do rzeczywistych potrzeb każdego członka firmy w myśl zasady „wiedzy potrzebnej". Zarazem oczekujemy ogólnej informacji, od której zależy bezpieczeństwo danej społeczności.

1.3. Poszukiwanie rozwiązań

Problem zapewnienia bezpieczeństwa (ogólnego, biznesowego, operacyjnego, fizycznego, technicznego, informacyjnego itd.) można wyrazić następująco: system idealny nie istnieje, ale mamy kilka sprawdzonych, bardzo dobrych rozwiązań…

Podstawą do takiej opinii jest rozwój metodologii w dziedzinie zabezpieczeń, który daje nam dostęp do szeregu otwartych metodyk krajowych (od ENSI Total Information Security Management – 1996 r. – do ENSI Total Security Management – 2004 r.) oraz zagranicznych (SW-CMM – 1991 r., SABSA – 1999 r.).



Rys. 2. Realizacja zabezpieczeń w obecnym układzie

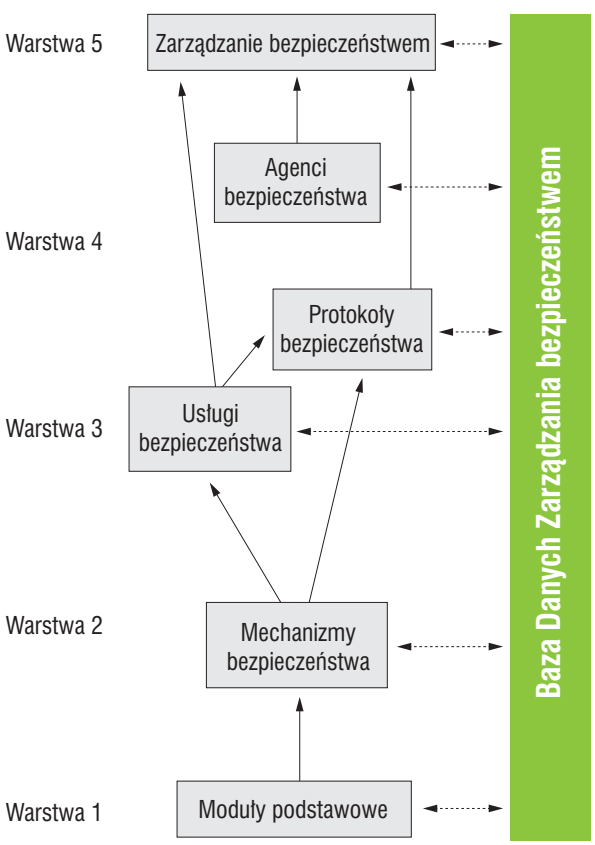
Każda z tych metodyk, uwzględniając w swej treści wymagania podstawowe i powiązania normatywne, które wynikają z „dobrych praktyk", traktuje jako nadrzędny cel zabezpieczanie chronionych zasobów w możliwie prosty i zarazem efektywny sposób (modelowo), z dopasowaniem praktycznych rozwiązań i zaleceń do rzeczywistych warunków działania.

Pod pewnymi względami nasze dotychczasowe działania ochronne przypominają postępowanie Holendrów, którzy na osuszonym dnie morskim (polderach) stawiają swoje budowle, świadomi konieczności ciągłego dozorowania wałów (rys. 2) i ciągłego zagrożenia zalaniem przez morze.

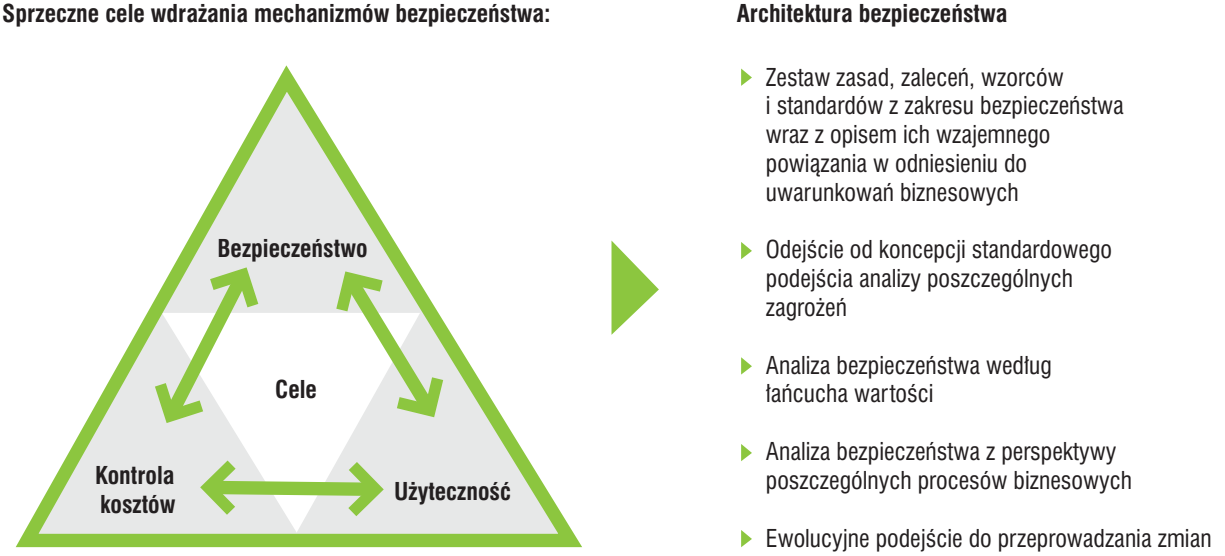
Odpowiada to sytuacji biznesowej, w której, świadomi zagrożeń i ich skutków, ryzykujemy posiadanymi zasobami, wychodząc z założenia, że potrafimy w pełni kontrolować zagrożenia i eliminować podatności. Niestety, skutki przeszacowania naszych własnych możliwości mogą być katastrofalne dla prowadzonego biznesu.

Problemem staje się nie tyle zbieranie wszystkich sygnałów o zagrożeniach, co ich analiza i segregacja według znaczenia i wagi potencjalnych skutków materializacji ryzyka. Obecnie istnieje potrzeba zarządzania bezpieczeństwem w trybie „półautomatycznym" z wykorzystaniem wielowarstwowego systemu sieci neuronowych, integrującego rozległe obszary podlegające ochronie i funkcjonującego automatycznie w zakresie wyuczonych procedur bezpieczeństwa.

Jak dotąd jest to teoretyczne rozwiązanie dla potrzeb sytemu zbudowanego w układzie sieci neuronowej, o zweryfikowanych elementach wykonawczych (informacje naukowe donoszą o uruchomionych rozwiązaniach prototypowych, testowanych na zlecenie DARPA DoD USA).



Rys. 3. Zintegrowane zarządzanie bezpieczeństwem



Rys. 4. Uwarunkowania architektury bezpieczeństwa

2. Współczesne wyzwania (terroryzm, bezpieczeństwo komunikacji i dostaw)

Współcześnie mamy do czynienia z różnymi zagrożeniami bezpieczeństwa obiektów, powodowanymi m.in. przez terroryzm, pospolitą przestępczość, szpiegostwo, sabotaż gospodarczy, nieporadność i beztroskę samych użytkowników obiektów. Zagrożenia mogą być powodowane także przez powiązania komunikacyjne i informacyjne – szczególnie w przypadku obiektów ruchomych.

Terroryzm stanowi istotne zagrożenie dla bezpieczeństwa Polski. Mówi o tym m.in. dokument *Strategia Bezpieczeństwa Narodowego RP* z 2007 roku – w punkcie 34 znajduje się następujący zapis: „Zagrożeniem dla Europy, w tym i dla Polski, jest zorganizowany terroryzm międzynarodowy. Polska musi się liczyć z możliwością działań skierowanych przeciwko niej w związku z udziałem w kampanii antyterrorystycznej. Nie można wykluczyć akcji odwetowych będących konsekwencją prowadzonych przez NATO lub UE operacji stabilizacyjnych i pokojowych".

Dr Jakub Jałoszyński[1] wśród czynników powodujących zagrożenie terroryzmem wymienia:

– prozachodnią politykę Polski i członkostwo w NATO oraz Unii Europejskiej,
– udział polskich żołnierzy w misjach pokojowych i stabilizacyjnych (m.in. w Iraku, Afganistanie, Jugosławii),
– strategiczne partnerstwo z USA oraz możliwość stacjonowania żołnierzy amerykańskich w Polsce,
– normalizację stosunków z Izraelem.

Nie można zapominać także o wkraczaniu tego zjawiska w nowe sfery – jak choćby cyberterroryzm, który wraz ze zwiększaniem się zależności od systemów informatycznych staje się coraz większym zagrożeniem dla bezpieczeństwa państwa.

Dodatkowym czynnikiem wpływającym na zwiększoną atrakcyjność naszego kraju jako potencjalnego celu ataku terrorystycznego jest organizowanie (wspólnie z Ukrainą) Euro 2012. Impreza sportowa tej rangi i o takiej skali przyciągnie uwagę mediów z całego świata, a chęć wzbudzenia zainteresowania mediów to jedna z cech współczesnego terroryzmu. Zamachy terrorystyczne w czasie imprez sportowych nie są niczym nowym. Po raz pierwszy zamach taki miał miejsce w 1972 roku, w czasie Igrzysk Olimpijskich w Monachium (Niemcy). Z kolei w czasie Igrzysk Olimpijskich w Atlancie (USA) w 1996 roku również miał miejsce zamach terrorystyczny, tym razem z użyciem ładunku wybuchowego. W wyniku eksplozji bomby (dla zwiększenia siły rażenia wypełnionej gwoździami i innymi metalowymi przedmiotami) zginęła jedna osoba, a ponad 100 zostało rannych. Warto pamiętać, że sprawcę tego zamachu udało się zatrzymać dopiero w 2003 roku(!).

Specyfika imprez sportowych realizowanych w dużych aglomeracjach miejskich wymaga zabezpieczenia środków komunikacji i zwalczania przestępczości pospolitej na ulicach i w środkach transportu. Zapewnianie bezpieczeństwa środków transportu jest elementem ochrony transportu gospodarczego i przeciwdziałania przestępstwom (napadom na TIR-y, włamaniom do kontenerów itp.). Ważna jest wielopunktowość łańcucha bezpieczeństwa (miejsce załadunku – trasa – postoje – miejsce docelowe – rozładunek), który obejmuje ruchome obwody zabezpieczające (patrole policji i straży miejsko-gminnych, ochronę parkingów). Odrębnym elementem jest ustawowy nadzór i wsparcie bezpieczeństwa konwoju w drodze wynikające z planów przemieszczania broni, materiałów niebezpiecznych, rzeczy wartościowych oraz dużych kwot pieniężnych (ŻW, PP, SUFO). Ponadto należy zwrócić uwagę na wymagania CTPAT związane z bezpieczeństwem ładunków transportowanych do USA (np. odprawa celna w Warszawie, skład cargo i fracht w Hamburgu), wynikające z zaleceń Custom Service USA.

Jak widać, ruchomość obiektów wymagających ochrony powoduje wiele nowych problemów związanych z potrzebą wypracowania metod i sposobów zapewnienia im bezpieczeństwa. Wiele kwestii wynika bezpośrednio ze stosowanej architektury bezpieczeństwa (rys. 4).

1) Materniak D., Polska w cieniu terroryzmu, 30.03.2010r, materiały Centrum Badań nad Terroryzmem Collegium Civitas, www.cbnt/psz/raporty

Rys. 5. Oddziaływania na bezpieczeństwo obiektu

3. Ujednolicanie reguł zarządzania bezpieczeństwem (informacja o obiekcie)

Podstawę działań na rzecz bezpieczeństwa obiektu stanowi informacja o jego aktualnym stanie, konfiguracji systemów i elementów ochronnych oraz występujących zagrożeniach. Wszystkie towarzyszące temu procesy główne (zarządzanie, eksploatacja, doskonalenie i utylizacja) są realizowane na bazie bezpiecznego przetwarzania informacji. Rozwiązania z tego zakresu są domeną SZBI/ISMS (Systemu Zarządzania Bezpieczeństwem Informacji/Information Security Management System) i obecnie są porządkowane przez wymogi JCTP1 ISO/IEC (SC27) dotyczące wspólnych regulacji w ramach rodziny norm 27000 (prace rozpoczęto w latach 2003–2004, normy ogłoszono jako przyjęte 15 kwietnia 2005 roku w Wiedniu).

Normy dotyczące zarządzania bezpieczeństwem informacji bazują na terminologii procesowej zawartej w normach ISO 9000 oraz zaleceniach systemowych wynikających ze stosowania cyklu stałego doskonalenia (koło Deminga – P-D-C-A), a jednocześnie uwzględniają zasady systemowego podejścia do badanych organizacji – zasady, które są szczególnie istotne ze względu na potrzeby analizowania pojawiających się nowych postaci ryzyka.

4. Podsumowanie konferencji

Konferencja zwróciła uwagę na to, że bezpieczeństwo w XXI wieku zależy od umiejętności zbierania, przetwarzania, przechowywania i wykorzystywania informacji generowanych przez poszczególne urządzenia lub systemy, których zadaniem jest zapewnienie ochrony osób, mienia (w tym przedmiotów jednostkowych o nieodtwarzalnej wartości) oraz danych.

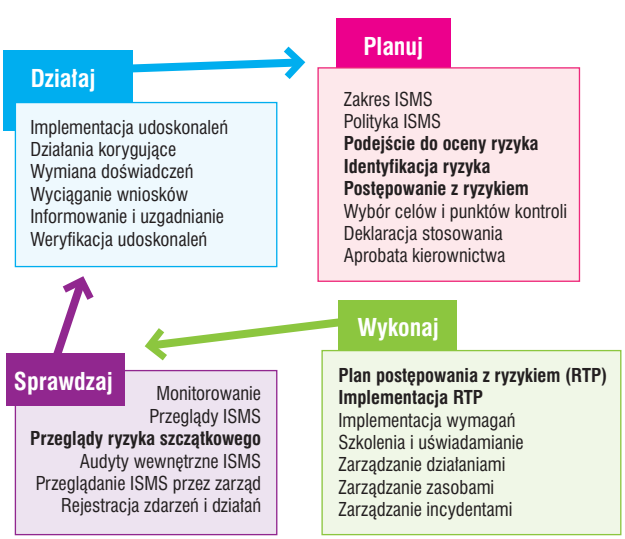
Należy zastanowić się:
- co jest punktem wyjścia i celem ochrony;
- jak wiele elementów składa się na poczucie bezpieczeństwa;
- **jakie ograniczenia mają wdrożone systemy;**
- jakie mamy możliwości logistyczne wobec wymagań ochronnych.

Pamiętajmy o tym, że:
- **„nie ma żadnych pewnych systemów, są tylko stopnie niepewności”;**
- **„aby zmniejszyć o połowę niepewność, należy podwoić koszt”.**

Konferencja wskazała obszar niezbędnych do podjęcia prac uzupełniających z zakresu istniejących oraz nowych i sygnalizowanych potrzeb obiektowych, bowiem współcześnie zabezpieczane obiekty zmieniają swoje charakterystyki (wielość elementów składowych, rozległość w terenie, ruchliwość), stawiając przed organizatorami ochrony nowe wymagania dotyczące nie tylko czasu i sposobu funkcjonowania samej ochrony bezpośredniej (fizycznej i technicznej), ale także systemów ostrzegania i powiadamiania o zagrożeniach.

W licznych referatach przedstawiono szerokie spektrum współczesnych zagadnień bezpieczeństwa (J. Mikulik – AGH; M. Byczkowski – ENSI), odniesiono się również do obowiązujących zależności prawnych (W. Kłusek, P. Januszewicz – Wojsko Polskie) oraz zakresu dobrowolnej normalizacji europejskiej i międzynarodowej (R. Grabiec – PKN). Liczne poszczególne zależności wobec zmieniających się wymagań omówiono z szerokiej perspektywy użytkowej (M. Blim – BURiK POLALARM) oraz społecznej (A. Białek – BZ WBK; K. Ciesielski – POLALARM). Pokazano też ich wycinkowe i specjalistyczne zastosowanie w dużych projektach europejskich (M. Patej – BIATEL), wskazując przy tym na coraz większe znaczenie poprawnie zrealizowanego audytu w zarządzaniu bezpieczeństwem (A. Wójcik – ATM).

Padające z sali pytania oraz kuluarowe wypowiedzi poszczególnych uczestników potwierdziły potrzebę i zasadność rozszerzenia wiedzy z tej skomplikowanej dziedziny. Funkcjonowanie z zachowaniem poprawności funkcji ochronnych na obszarze Schengen (zgodność w ramach Europejskiego Obszaru Gospodarczego – *European Economic Area*) jest związane z koniecznością przestrzegania norm europejskich i dodatkowych wymagań kontraktowych. Zbliżające się masowe imprezy (m.in. Euro 2012) to dla Polski nieuchronny sprawdzian ze sprawności ochrony wielu różnorodnych obiektów (stałych i komunikacyjnych, małych i bardzo dużych) w warunkach trudnych do przewidzenia zagrożeń (zewnętrznych i wewnętrznych).



Rys. 6. Postępowanie z ryzykiem w cyklu Deminga SZBI/ISMS

Podsumowanie

Zwrócenie uwagi na konieczność podzielenia się doświadczeniami z zakresu zarządzania bezpieczeństwem, a także na problem zmian w samych strukturach obiektów oraz ich charakterze funkcjonowania potwierdza zasadność zorganizowania konferencji.

Opracował: dr inż. Marek Blim

Informatyka śledcza

czyli jak ochronić firmę przed nieuczciwymi pracownikami

Paweł Odor

Kradzież firmowych dokumentów, nielegalne kopiowanie danych bądź przekazywanie poufnych klauzul i umów konkurencji za pomocą komputera to tylko niektóre z praktyk, jakich coraz częściej dopuszczają się nieuczciwi pracownicy tysięcy krajowych i międzynarodowych firm. Niestety także w Polsce nieuczciwe działania byłych lub obecnych pracowników wykorzystujących firmowe komputery bądź inne urządzenia elektroniczne zdarzają się coraz częściej. Jak więc ochronić naszą firmę przed poważnymi stratami finansowymi, jakie generują przestępcy komputerowi? Rozwiązaniem jest mało jeszcze znana w Polsce dziedzina IT – informatyka śledcza

Jak wskazują specjaliści, według raportów firm monitorujących nadużycia w biznesie, do których należą także przypadki wycieku strategicznych danych, na przestrzeni lat 2006–2009 firmy z dziesięciu największych sektorów gospodarki światowej straciły średnio 8,2 miliona dolarów w wyniku nieuczciwych zachowań pracowników własnych bądź konkurencji. Również w Polsce w wyniku tego typu zdarzeń firmy tracą ogromne sumy. Choć nie ma szczegółowych danych dotyczących strat polskich firm (m.in. dlatego, że same firmy rzadko przyznają się do tego, iż padły ofiarą takich działań), szacuje się, że straty te mogą być liczone w milionach złotych.

Rozwiązaniem mogącym pomóc przedsiębiorstwom jest wprowadzenie procedur i odpowiedniej polityki bezpieczeństwa danych, która pozwala na odpowiednią reakcję w momencie zaistnienia incydentu. Do kogo zwrócić się w tego typu sytuacjach? W przypadku podejrzenia nadużycia związanego z nieuczciwym zachowaniem pracowników najlepiej skorzystać z usług informatyków śledczych – elektronicznych detektywów – którzy pomogą przeprowadzić wewnętrzne śledztwo, analizując firmowe urządzenia, a następnie dostarczą elektronicznych środków dowodowych, które firma będzie mogła wykorzystać w sądzie. Jak wyglądają więc działania informatyków śledczych w Polsce i na świecie?

Czym jest informatyka śledcza?

Informatyka śledcza (ang. *computer forensics*) polega na dostarczeniu elektronicznych środków dowodowych dla firm, instytucji bądź osób prywatnych, które następnie zostaną wykorzystane przez odpowiednie organa prawne. Jest to więc zespół działań i czynności specjalistów, które polegają na zabezpieczeniu, przeszukiwaniu i wykrywaniu dowodów nadużyć i przestępstw dokonanych z użyciem komputera lub innych urządzeń elektronicznych. Dzięki informatyce śledczej możemy więc odtworzyć kolejność zdarzeń użytkownika urządzenia elektronicznego w czasie (i odpowiedzieć na pytania: „kto?", „co?", „gdzie?", „kiedy?", „jak?"), działając na podstawie informacji niedostępnych dla użytkowników i administratorów systemu.

By w pełni zrozumieć, czym zajmuje się informatyka śledcza, konieczne jest wcześniejsze zapoznanie się z procesem zapisywania danych w naszych komputerach. Generują one bowiem znacznie więcej informacji, niż zdajemy sobie z tego sprawę, przy czym wiele z nich jest wymaganych do prawidłowej pracy systemu i nie są one dostępne dla użytkowników. Dotyczy to np. metadanych, a więc informacji opisujących inne informacje, których interpretacja wymaga odpowiedniej wiedzy i doświadczenia. Pozostałe dane spoczywają w różnych obszarach nośników danych w postaci logów, rejestrów i ukrytych plików systemowych. Oczywiście w kontekście rozwoju technologii mobilnych należy wspomnieć także o analizie telefonów komórkowych (ang. *mobile forensics*), których pamięci coraz częściej zawierają istotne dla naszych firm dokumenty.

Najpopularniejszymi nośnikami dowodów elektronicznych trafiającymi do 32 laboratoriów firmy Kroll Ontrack są dyski twarde komputerów osobistych (61,5%), serwery (20%, w tym serwery pocztowe – 7% – oraz pozostałe serwery, np. zapisujące dane z kamer monitorujących ulice – 13%), notatniki elektroniczne (3%), pamięci przenośne (11%) oraz telefony (2,5%). Większość serwerów trafia do ekspertyzy wraz z kopiami bezpieczeństwa.

Polityka bezpieczeństwa danych – klucz do sukcesu

Aby zabezpieczyć firmę, należy zacząć od stworzenia odpowiedniej polityki bezpieczeństwa danych. Pozwoli ona zabezpieczyć się nie tylko na wypadek wycieku danych spowodowanego przez nieuczciwych pracowników, lecz także na wypadek awarii sprzętu lub przypadkowego skasowania danych.

Odpowiednia polityka bezpieczeństwa staje się coraz bardziej znaczącym elementem strategii firm, co jest widoczne również w naszym kraju. Najlepiej ze wszystkich firm wypadają na tym tle oddziały zachodnich koncernów – tam odpowiednie procedury już są wdrożone. Według szacunków w ciągu najbliższych lat informatyka śledcza stanie się stałym elementem polityki bezpieczeństwa w wielu dużych polskich firmach oraz w części firm z sektora MSP. Bardzo ważne jest tutaj zdobycie wiedzy dotyczącej wykorzystania elektronicznych środków dowodowych na potrzeby zwalczania nadużyć w biznesie.

Jeśli chodzi o dane wykorzystywane przez sądy jako elektroniczne środki dowodowe, z obserwacji ekspertów firmy wynika, że zawsze lepiej postrzegane jest działanie podmiotu niezależnego, który nie będzie czerpał korzyści z ewentualnego postępowania wtedy, gdy dowody rzeczywiście staną się potrzebne. Zabezpieczenie danych przez zewnętrznych specjalistów w obecności odpowiednich osób reprezentujących firmę i ewentualnie prokuraturę lub policję jest rozwiązaniem optymalnym. Rolą procedur firmowych w tym procesie powinno być odpowiednio wczesne wykrycie nadużycia, a następnie działania, które będą zmierzały do zabezpieczenia, a nie zatarcia śladów. To właśnie wskutek niewłaściwego postępowania nie można wykorzystać wielu śladów, często oczywistych, w formie dowodów elektronicznych.

Z wielu względów włączenie procedur informatyki śledczej do polityki bezpieczeństwa stanie się w przyszłości motorem rozwoju w firmach specjalizujących się w informatyce śledczej. Po pierwsze firmy te mają już doświadczenie, przeszkolonych specjalistów oraz odpowiednie zaplecze sprzętowe i programowe. Ponadto niektóre firmy będą w stanie zabezpieczyć dowody wewnętrznie, natomiast ich ewentualną analizą będą się zajmować eksperci z tej dziedziny.

Prócz tego, eksperci w dziedzinie informatyki śledczej będą mieli za zadanie pomoc w tworzeniu i szkoleniu personelu wewnętrznych działów informatyki śledczej. Stworzenie komórki wyspecjalizowanej w informatyce śledczej nie jest jednak tanie.

Rys. 1. Proces informatyki śledczej

Dlatego nadal większość firm działających na rynku, mając wdrożone procedury informatyki śledczej, w przypadku wychwycenia incydentu będzie korzystała z pomocy fachowców z zewnątrz.

Informatyka śledcza jest najbardziej rozwinięta w USA i krajach Europy Zachodniej. Stosowanie dowodów elektronicznych jest powszechną praktyką w przedsiębiorstwach. W tym przypadku mamy do czynienia z wysoką świadomością firm. Typowym działaniem w korporacjach działających w krajach najbardziej rozwiniętych jest m.in. zabezpieczanie danych z komputera pracownika, który zmienia pracę. Takie działanie ma na celu zabezpieczenie interesów obu stron, pracownika i firmy. Określa stan faktyczny w momencie zakończenia współpracy pracownika z firmą oraz wiarygodnie dokumentuje jego działania na rzecz organizacji.

W zdecydowanej większości przypadków informatyką śledczą zajmują się niezależni eksperci. Jest to szczególnie istotne w USA, gdzie taka niezależność jest szczególnie istotna. Rozwiązania amerykańskie często bywają wzorem dla działań z zakresu informatyki śledczej w innych krajach, oczywiście z uwzględnieniem uwarunkowań prawnych danego kraju.

Proces informatyki śledczej

Proces informatyki śledczej składa się z pięciu etapów: zbierania informacji, wyliczenia sumy kontrolnej, odzyskania danych, ich analizy oraz stworzenia raportu z przeprowadzonych działań.

Zgromadzenie dowodów polega m.in. na zabezpieczeniu nośników danych i stworzeniu dwóch kopii każdego nośnika, które wykorzystują informatycy śledczy, szukając dowodów winy podejrzanego. Każdy z etapów pracy musi być udokumentowany tak, aby przedstawiony materiał nie utracił wartości dowodowej, dlatego też tak istotna jest tutaj obecność profesjonalistów korzystających z najnowocześniejszych narzędzi.

Wynikiem pracy informatyków śledczych jest szczegółowy raport zawierający informacje o odnalezionych danych, istotnych dla prowadzonej sprawy. Elementem raportu powinno być także osadzenie kluczowych zdarzeń w czasie. Jako że treść raportu musi być ściśle skorelowana ze sprawą, konieczna jest bliska współpraca specjalistów z laboratorium i osób prowadzących sprawę. Elementem współpracy laboratorium informatyki śledczej i klienta jest także przedstawianie wyników prac w sądzie. Informatycy śledczy,

Najciekawsze i najpoważniejsze przypadki działań informatyków śledczych w Polsce i na świecie

Sprawa gdańskiej gimnazjalistki

Działania związane z informatyką śledczą dotyczą nie tylko danych umieszczonych na dyskach twardych komputerów, ale również w takich urządzeniach, jak pamięci flash bądź telefony komórkowe.

W związku ze zwiększającą się liczbą funkcji i pojemnością telefonów komórkowych pochodzące z nich dane mogą stać się cennym źródłem dowodowym, wykorzystywanym w informatyce śledczej. Jednym z takich przypadków była udana próba odzyskania filmu zapisanego w pamięci telefonu komórkowego jednego z gdańskich uczniów w roku 2006.

Film ten był zapisem napastowania jednej z gimnazjalistek przez grupę jej kolegów, w tym chłopca nagrywającego to zdarzenie, podczas lekcji w szkole. Nagranie zostało następnie opublikowane w Internecie. Po tym zdarzeniu i rozgłosie, jaki został mu nadany w mediach, chłopcy skasowali film. Telefon został jednak zabezpieczony przez policję, której przedstawiciele w toku postępowania przekazali aparat do analizy specjalistom informatyki śledczej. W laboratorium odzyskano wykasowaną zawartość telefonu, w tym nagranie z lekcji. Film został wykorzystany w sprawie.

Komputer prezesa portalu wp.pl

Sprawa komputera prezesa Wirtualnej Polski jest przykładem straty, jaką poniosła jedna ze stron z powodu braku świadomości istnienia usług informatyki śledczej w Polsce.

Większościowy udziałowiec portalu wp.pl zawarł porozumienie z posiadaczami udziałów stanowiącymi mniejszość, w którym zobowiązał się do odkupienia reszty udziałów po określonym czasie. Cena wykupienia udziałów miała zależeć bezpośrednio od liczby użytkowników portalu.

Po upływie terminu, w którym miało nastąpić odkupienie udziałów, okazało się, że mniejszościowy pakiet udziałów jest droższy niż łączna kapitalizacja dwóch najbardziej konkurencyjnych portali.

Większościowy udziałowiec wycofał się ze zobowiązania. Podjęto działania prowadzące do pogorszenia finansowej kondycji portalu, a w konsekwencji do jego upadłości. Mniejszościowi udziałowcy zdecydowali się na zweryfikowanie zawartości przenośnego komputera jednego z managerów.

Komputer zawierający dane, które miały stanowić materiał dowodowy w sprawie, zdeponowano u notariusza. Zanim to jednak nastąpiło, osoby te otworzyły pliki, w których znajdowały się strategiczne dla sprawy informacje – materiały mające świadczyć o próbie doprowadzenia portalu do upadłości. Niestety, otwierając dokument, zmieniono jego atrybuty, włącznie z datą utworzenia, pozbawiając go wartości dowodowej.

Gdyby mniejszościowi udziałowcy zlecili takie działania informatykom śledczym, zabezpieczyliby oni nośnik, wykonaliby kopię jego zawartości bez uruchamiania plików oraz umożliwiliby osobom prowadzącym dochodzenie wgląd do zawartości plików. W ten sposób wartość dowodowa zgromadzonego materiału zostałaby zachowana.

Informatycy śledczy dla FBI i Prokuratora Generalnego USA

W Stanach Zjednoczonych pracownikowi dużej korporacji została wytoczona sprawa o umyślne spowodowanie utraty strategicznych danych jego pracodawcy. Miało to doprowadzić do znacznych strat firmy, a w rezultacie do zwolnienia jej 100 pracowników.

W trakcie analizy dokonywanej przez informatyków śledczych okazało się, że jeszcze pracując w korporacji, pracownik stworzył program komputerowy, który niszczył dane. Program umieścił na firmowym serwerze. Okazało się, że narzędzie działało na zasadzie bomby zegarowej. „Bombę" aktywował

przywołani przez prokuratora i sądy w celu wydania opinii, prezentują materiał dowodowy jako tzw. biegli *ad-hoc*. Pomimo tego, że nie wszystkie sprawy trafiają na wokandę, wszystkie czynności w ramach procesu informatyki śledczej muszą być wykonane w taki sposób, aby wartość dowodowa zgromadzonego materiału była niepodważalna. Na świecie tylko około 20 procent spraw, którymi zajmują się specjaliści informatyki śledczej, ma swój finał w sądzie. Często potrzebne są jedynie dowody winy pracownika, pozwalające pracodawcy na uszczelnienie systemu dostępu do informacji.

W kryzysie i nie tylko…

Działania informatyków śledczych są szczególnie istotne w okresach, w których nasilają się zwolnienia w różnych sektorach gospodarki. Przykładem takiego okresu jest choćby ostatni światowy kryzys, który odcisnął swe piętno na niemal każdej branży. Gdy każdego dnia liczba zwalnianych pracowników rosła, pozbawione zabezpieczeń firmy stanęły w obliczu utraty swych kluczowych zasobów. Dodatkowym problemem stało się także ryzyko nadużyć, które mogli popełnić pracownicy, których wynagrodzenia zostały znacznie zmniejszone. Światowy kryzys jest tylko przykładem, lecz podobnie może być w przypadku pojedynczej firmy, która ma tymczasowe problemy finansowe lub kadrowe. W takich przypadkach przedsiębiorstwa są narażone na utratę nie tylko swych środków, lecz także budowanego przez lata wizerunku.

Należy pamiętać, że oprócz nadużyć pracowników w związku z panującym w firmie kryzysem należy spodziewać się także większej liczby przypadków kradzieży własności intelektualnej – technologii, autorskich rozwiązań, strategii czy planów – a także szpiegostwa przemysłowego, przejmowania doświadczonych pracowników czy powstania układów gospodarczych łamiących prawo. Warto zauważyć, że nawet w okresie dobrej koniunktury sama tylko wzmianka o nadużyciach w firmie powoduje spadek wartości jej akcji. Oczywiście w przypadku kryzysu spadek ten może być większy.

Paweł Odor

Autor jest głównym specjalistą polskiego oddziału Kroll Ontrack, największej i najdłużej działającej firmy zajmującej się informatyka śledczą i odzyskiwaniem danych na świecie.

nieświadomie jeden z pracowników, logując się po określonym czasie na tym serwerze.

Specjaliści wykazali winę zwolnionego pracownika, obalając główny argument obrony, jakoby dane firmowe zostały skasowane przypadkowo. Wykazali dodatkowo, że na prywatnym komputerze oskarżonego znajdowały się dane identyczne z tymi, które posłużyły do stworzenia groźnego programu. Po analizie wszystkich danych znajdujących się na serwerach pocztowych oraz koncie pocztowym podejrzanego pracownika informatycy śledczy przedstawili materiał dowodowy w sądzie. Dopiero te działania umożliwiły udowodnienie winy pracownika.

Dysk Aleksandry Jakubowskiej i dyski wykradzione z MSZ

Do końca lat dziewięćdziesiątych świadomość istnienia informatyki śledczej była w Polsce niemalże zerowa. Zmiany nastąpiły dopiero wtedy, gdy działania związane z informatyką śledczą zaczęły dotyczyć głośnych spraw, takich jak np. afera Rywina czy wykradzenie dysków z Ministerstwa Spraw Zagranicznych. Jednocześnie wydarzenia te pokazały, jak istotna może okazać się praca specjalistów informatyki śledczej.

W roku 2002 rozpoczęło się śledztwo związane z tzw. aferą Rywina. Jednym z kluczowych dla śledztwa działań było odzyskanie wiadomości pocztowej ze sformatowanego dysku minister Aleksandry Jakubowskiej. Znajdowały się na nim dowody pozwalające prokuraturze na ustalenie przebiegu wydarzeń w jednym z wątków afery korupcyjnej.

Drugim wydarzeniem, które zwróciło uwagę opinii publicznej na informatykę śledczą, było wykradzenie dysków z Ministerstwa Spraw Zagranicznych. Brak zabezpieczenia zużytych nośników i monitorowania dostępności do nich mógł, w najgorszym wypadku, doprowadzić do pogorszenia stosunków międzynarodowych między Polską a innymi krajami.

Nieuczciwi pracownicy

Ostatnio coraz powszechniejszy staje się problem nieuczciwości pracowników. Do najliczniejszych przypadków, którymi zajmują się elektroniczni detektywi, należy m.in. kradzież danych przez nieuczciwych pracowników.

Przykładem jest jedna z firm informatycznych, zajmująca się tworzeniem i wdrożeniami aplikacji biznesowych. Zespół zatrudniony do obsługi jednego z klientów firmy postanowił przejąć proponowane przez firmę rozwiązania (przygotowywał się do kradzieży kodu źródłowego informacji) i sprzedać je poza nią, po uprzednim zwolnieniu się poszczególnych osób z pracy. Ustalono nawet osobną pulę pieniędzy, która miała być przeznaczona na ewentualną karę nałożoną przez pracodawcę. Propozycję, która miała być tańsza od oryginalnej, złożył jeden z handlowców, będący w bezpośrednim kontakcie z klientem. W efekcie klient postanowił zerwać umowę z firmą i skorzystać z tańszej oferty, złożonej przez nieuczciwych pracowników.

Zaniepokojony takim postępowaniem klienta zarząd firmy postanowił przeanalizować zaistniałą sytuację i w wyniku własnych ustaleń dotyczących handlowca zdecydował się na dalsze kroki – zlecenie firmie zajmującej się informatyką śledczą analizy komputerów, urządzeń PDA oraz telefonów komórkowych należących do zespołu. Efekty pracy specjalistów w pełni ukazały nieuczciwe działania pracowników i pozwoliły firmie na wyciągnięcie prawnych konsekwencji w stosunku do zaangażowanych w nie osób.

Dostarczenie elektronicznych środków dowodowych do trzech krajów jednocześnie

Eksperci największej firmy zajmującej się informatyką śledczą na świecie otrzymali zlecenie tzw. akwizycji danych, polegającej na skopiowaniu informacji elektronicznych w taki sposób, aby nie straciły one wartości dowodowej (narzędzia wykorzystywane przez informatyków śledczych pozwalają na zachowanie tzw. sumy kontrolnej; jej niezmieniona wartość gwarantuje brak ingerencji w zawartość zabezpieczanych plików elektronicznych). W tym samym czasie identyczną operację przeprowadzili specjaliści informatyki śledczej z tej samej firmy w Niemczech i we Francji. Zleceniodawcą był zarząd francuskiej firmy farmaceutycznej.

Powodem zatrudnienia elektronicznych detektywów było podejrzenie o malwersacje finansowe zarządu polskiego oddziału

firmy, którego członkowie otworzyli firmę pośredniczącą w zakupach dla koncernu, oferując towary po cenach nierynkowych i powodując w ten sposób wymierne straty firmy.

Operacja zebrania materiałów dowodowych, przeprowadzana w każdym z trzech krajów tej samej nocy, odbyła się w obecności prawnika, notariusza i pracownika firmy ochrony. Informatycy śledczy skopiowali dane z każdego komputera w firmie oraz z urządzeń służących do archiwizacji firmowych danych. Każde z miejsc pracy zostało sfotografowane.

Dane z Niemiec i Polski trafiły następnie do Francji. Podobnie jak dane z siedziby głównej koncernu, zostały poddane analizie. Wynikało z niej, że przypuszczenie działania zarządu polskiego oddziału firmy na szkodę koncernu jest prawdziwe.

Po analizie wyników zarząd francuskiego koncernu zdecydował się na zmianę całego personelu polskiego oddziału (zarządu i pracowników). Nie wiadomo, czy członkom zarządu wytoczono procesy.

Kradzież i wykorzystanie danych przez konkurencję

Udostępnianie danych osobom, które tworzą określone projekty dla danej firmy, może niekiedy okazać się niezwykle ryzykowne. Doświadczyło tego jedno z największych biur projektowych, które na potrzeby realizacji jednego ze zleceń postanowiło podjąć współpracę z inną firmą. Miała ona wesprzeć działania biura i wraz z jego pracownikami utworzyć zespół zajmujący się projektem przez następne czternaście miesięcy.

Powołany zespół pracował w siedzibie biura projektowego (zleceniodawcy). Dzięki temu pracownicy firmy wspomagającej biuro mieli potencjalną szansę na bezprawny dostęp do wszelkich danych znajdujących się na komputerach ich zleceniodawcy.

W trakcie realizacji projektu pracownicy biura przypadkowo odkryli, iż na rynku pojawiły się produkty bazujące na rozwiązaniach technologicznych stworzonych przez nich samych. W tej sytuacji, obawiając się przecieku, przeprowadzono analizę komputerów pracowników, serwerów danych oraz przesyłanych dokumentów. Pozwoliło to na ustalenie źródła przecieku, którym okazał się zespół projektowy, a dokładnie jeden z pracowników firmy zatrudnionej przez biuro. Ustalono, że kilkakrotnie włamywał się on na serwery, gdzie przechowywane były dane pochodzące z innych projektów, po czym przesyłał je na serwery swej macierzystej firmy.

Odkrycie tych działań nie byłoby możliwe bez dokonanej przez specjalistów szczegółowej analizy komputerów biura projektowego i poprawnego zabezpieczenia elektronicznych środków dowodowych, które mogły być użyte w sądzie. Przypadek ten pokazuje zarazem, jak istotne jest zabezpieczenie danych firmy, których wykorzystanie może być w przyszłości przyczyną jej poważnych problemów.

Komputer wyrzucony z okna

Dane z odzysku mogą być i bywają dowodami przestępstw. Osoby, które łamią prawo, pilnie strzegą informacji mogących je pogrążyć.

Ponieważ wiele takich danych jest archiwizowanych na komputerach (często przenośnych), jedną z metod działania prowadzącego do oskarżenia przestępcy jest zgromadzenie elektronicznych dowodów łamania prawa, czyli danych zapisanych w formie elektronicznej.

Przestępcy najczęściej korzystają z komputerów przenośnych. Pozwala to im na ciągły nadzór nad ważnymi danymi.

W razie potrzeby jest też łatwiej pozbyć się notebooka niż setek lub tysięcy kartek papieru. Tak przynajmniej sądził ścigany przez policję przestępca, księgowy jednej z dużych grup przestępczych. Uciekając po schodach budynku, dotarł na dach i zrzucił z niego przenośny komputer z obciążającymi go danymi.

Ponieważ informacje te mogły być decydujące w śledztwie, do odzyskania danych zatrudniono firmę specjalizującą się w informatyce śledczej. Po upadku cały komputer był mocno zniszczony. Jednak z uszkodzonego dysku udało się odzyskać około siedmiu procent danych. Taka ilość informacji wystarczyła do obciążenia podejrzanego.

Elektroniczne dowody fałszerstw

Do firmy zajmującej się informatyką śledczą trafiło zgłoszenie przesłane przez prokuraturę prowadzącą śledztwo w sprawie fałszowania dokumentów.

Podczas przesłuchań trzy zatrzymane osoby posługujące się sfałszowanymi dokumentami przyznały się do winy. Jednocześnie okazało się, że współpracował z nimi informatyk, który przygotowywał kopie dokumentów tożsamości, zaświadczeń o zatrudnieniu i pieczątek – wszystko to w wersji elektronicznej.

Po zeznaniu prokuratura wydała nakaz aresztowania podejrzanego o fałszerstwo oraz nakazała zarekwirowanie sprzętu komputerowego, z użyciem którego dokonywano fałszerstw.

Na porę zatrzymania podejrzanego wybrano wieczór. W czasie interwencji funkcjonariuszy fałszerz dokumentów próbował zniszczyć komputer, uderzając nim o ziemię. Jego działania odniosły skutek, ponieważ dysk twardy, który znajdował się w jego laptopie, uległ uszkodzeniu fizycznemu – jego elementy mechaniczne zostały uszkodzone.

W takim przypadku jedynym możliwym sposobem odzyskania danych jest otwarcie nośnika w laboratoryjnych warunkach oraz wykorzystanie technologii umożliwiającej odtworzenie danych bezpośrednio z otwartego nośnika.

W przypadku fałszerza informatycy śledczy odzyskali 74 pliki zawierające wzorce spreparowanych dokumentów. Informacje te posłużyły jako materiał dowodowy w prowadzonym przez prokuraturę dochodzeniu.

Była pracownica oskarżona o przyczynienie się do upadku firmy

Pracownica jednej z katowickich firm założyła własną firmę podczas trwania stosunku pracy. Bankrutujący pracodawca obwinił ją o problemy swojej firmy, które miały być spowodowane tym, iż pracownica wykonywała w czasie pracy czynności związane z działalnością jej prywatnej firmy, zaniedbując obowiązki służbowe.

Pracownica twierdziła, że wszystkie czynności związane z funkcjonowaniem swojej firmy wykonywała po pracy. Jako dowód zleciła analizę operacji wykonywanych z użyciem komputera elektronicznym detektywom – informatykom śledczym, którzy przeanalizowali dane znajdujące się w komputerze pracownicy. Okazało się, że kobieta wykonywała wszystkie czynności związane z prowadzeniem własnej firmy po godzinach pracy. Pracodawca odstąpił od skierowania sprawy do sądu.

Paweł Odor
Kroll Ontrack

Sygnalizatory z komunikatami głosowymi

światło i dźwięk dla bezpieczeństwa

SG-Pgw

- montowane przez puszkę PIP-3A

SGO-Pgz

- lampa ksenonowa z podwójnym błyskiem
- montowane przez puszkę PIP-4A

W2 lider w produkcji sygnalizatorów do systemów sygnalizacji pożaru.

Dane adresowe:
W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel./fax (052) 584 01 92
tel. (052) 345 45 00
biuro@w2.com.pl

Wewnętrzne i zewnętrzne **sygnalizatory z komunikatami głosowymi** firmy W2 jako jedyne tego typu urządzenia na rynku **uzyskały certyfikaty i świadectwa dopuszczenia CNBOP**. Wyróżniają je cechy takie jak możliwość wgrywania **do 4 dowolnych komunikatów**, synchroniczna praca w sieci. Sygnalizatory SGO-Pgz i SG-Pgw umożliwiają ponadto **proste adresowanie komunikatów** i współpracę z wyłącznikiem sygnału dźwiękowego WSD-1. Posiadają również przydatne funkcje takie jak ustalenie priorytetu komunikatów i zabezpieczenie przed utratą synchronizacji.

Więcej informacji na stronie **www.w2.com.pl**

STUDIUM AUDYTÓW BEZPIECZEŃSTWA INFORMACJI

CZYLI NIEPRAWIDŁOWOŚCI W OCHRONIE INFORMACJI (CZĘŚĆ II)

W części pierwszej artykułu zostały poruszone problemy związane z organizacją ochrony informacji w organizacji. Przedstawione zostały błędy, jakie popełniają organizacje podczas wdrażania zasad bezpieczeństwa informacji - błędy natury organizacyjnej lub wynikające z samego podejścia do problemu. W tej części skupimy się na równie prostych, oczywistych i niestety wciąż powtarzanych błędach, tym razem związanych z techniczną stroną realizacji koncepcji ochrony informacji i z konkretnymi działaniami mającymi na celu bezpieczeństwo informacji

Krzysztof Sierota

Analiza zagrożeń

Najpierw należy określić, co, dlaczego i jak chronić, gdyż – w największym uproszczeniu – do tego sprowadza się proces analizy zagrożeń. Uznany standard zarządzania bezpieczeństwem, określony w normie ISO 27001, wskazuje analizę zagrożeń jako podstawę zarządzania bezpieczeństwem informacji.

Jak jest w praktyce? Bardzo często organizacje nie wiedzą nawet, że należy przeprowadzić taką analizę, nie mówiąc o wykorzystaniu jej wyników. Prawie zawsze efektem jest słaba, pełna luk i niekompletna ochrona:

– brak inwentaryzacji zasobów informacyjnych, który często prowadzi do tego, że część wrażliwych aktywów informacyjnych pozostaje niechroniona;
– brak wiedzy o obecnych i potencjalnych zagrożeniach, która jest podstawą analizy (efektem jest słabe przygotowanie na wypadek naruszenia bezpieczeństwa informacji);
– brak wiedzy o rzeczywistych skutkach, możliwych stratach w przypadku naruszenia bezpieczeństwa informacji (często dopiero analiza zagrożeń pokazuje, że pewne straty są nie do zaakceptowania i organizacja musi im zapobiegać);
– niewłaściwy dobór zabezpieczeń, zbyt rygorystyczna lub zbyt liberalna ochrona informacji (efektem jest występowanie ewidentnych luk w zabezpieczeniach lub po prostu brak tych zabezpieczeń; innym efektem są zabezpieczenia zbyt rygorystyczne – nieadekwatne do stopnia zagrożenia) lub po prostu wybór bardzo drogich rozwiązań (np. kaskadowych haseł lub skomplikowanych i niepraktycznych procedur postępowania).

Istotny jest również aspekt ekonomiczny. Trudno mówić

o racjonalnym zarządzaniu zasobami, podejmowaniu decyzji dotyczących działań w dziedzinie bezpieczeństwa informacji, gdy brakuje rzetelnej analizy zagrożeń. Może zamiast kupować nowy, drogi serwer o większej wydajności lepiej wysłać administratorów na szkolenia, by umieli optymalnie wykorzystać to, czym dysponują?

Procedury i instrukcje

Precyzja i klarowność w opisie to klucz do tego, by zdefiniowane i udokumentowane procedury były stosowane przez pracowników. Niestety, często można mieć wiele zastrzeżeń do jakości dokumentacji. Chyba najlepszymi królikami doświadczalnymi do testowania zrozumiałości procedur są audytorzy, którzy, jako osoby z zewnątrz, zapoznają się z nimi i muszą je szybko zrozumieć, zapamiętać oraz wykorzystać podczas audytu. Jeżeli audytor nie rozumie, o co chodzi w danej polityce, procedurze, instrukcji, i musi ją kilkakrotnie przestudiować, to należy się spodziewać, że taki sam problem będzie miał przeciętny pracownik. A ponieważ nikt z nas, pracowników, nie ma czasu na studiowanie zawiłych instrukcji i procedur, zwykle nikt ich nie zna. Gorzej, jeśli większość z tych dokumentów jest właśnie taka…

Najważniejsze zarzuty pod adresem dokumentacji to:

– obszerność procedur i instrukcji (najlepiej funkcjonują krótkie, nawet jedno- czy dwu stronicowe dokumenty – łatwo je zapamiętać, a nawet wydrukować i powiesić na ścianie);
– „życzeniowy" charakter procedur/instrukcji (organizacje przedstawiają w dokumentacji idealny sposób postępowania, który nie może być realizowany w praktyce – lepiej opracować prostą, skromną, elastyczną procedurę);
– brak konsultacji z wykonawcami procedur/instrukcji (w efekcie ich realizacja jest dla wykonawców trudna lub wręcz niemożliwa, przyczyną jest brak współpracy departamentów bezpieczeństwa, oficerów i administratorów bezpieczeństwa z resztą organizacji);
– brak precyzji (nie wiadomo, kogo i czego dotyczy procedura, kto i kiedy powinien ją stosować; nagminnie używa się sformułowań typu „zaleca się, by kopie zapasowe były wykonywane […]", „powinno się"; to oczywiste, że wiele osób traktuje tak sformułowaną instrukcję jako wyłącznie życzliwą radę i postępuje według swoich przekonań, dlatego znacznie lepiej jest jasno i twardo formułować wymagania, np. „kopie zapasowe muszą być wykonywane […]").

Jeżeli jest to możliwe, należy zebrać najważniejsze wymagania dotyczące ochrony informacji w krótkim poradniku. Kilkustronicowy dokument zwykle wystarcza i może zawierać wszystkie informacje, które są potrzebne pracownikowi na co dzień. Pracownicy cenią sobie takie „ściągawki". Praktyka audytowa pokazuje, że świetnie się sprawdzają.

Uświadamianie

Jak głosi teoria i potwierdza praktyka, bezpieczeństwo informacji zależy od odpowiednio wyedukowanych pracowników, którzy wiedzą, czym jest ochrona informacji i jakie są jej cele.

Niestety, w praktyce obszar bezpieczeństwa informacji kojarzy się pracownikom z niepotrzebnymi, skomplikowanymi hasłami dostępowymi, ograniczeniami dostępu do danych i aplikacji, nudnymi szkoleniami dotyczącymi wyimaginowanych zagrożeń. Ogólnie jest to dla nich „zawracanie głowy". I mają rację.

Przede wszystkim konieczna jest zmiana podejścia pracowników, uświadomienie im potrzeby tego wszystkiego, co ma na celu bezpieczeństwo. Muszą wiedzieć, dlaczego chronimy informacje i jakie są konsekwencje braku ochrony. Warto przedstawić to obrazowo –przedstawić incydenty we własnej i innych organizacjach. Można zademonstrować, co można zrobić z zawirusowanym, zdalnie zarządzanym komputerem. Jeden z klientów, nie uprzedziwszy pracowników, po prostu wyłączył swoje systemy IT, aby zasymulować potężną awarię. Pracownicy dowiedzieli się, że była awaria i wszystko przepadło – muszą radzić sobie bez komputerów i serwerów. Z tego powodu nagle uświadomili sobie ważność ochrony informacji.

Co do edukacji – w trakcie szkoleń pamiętajmy, że dla większości pracowników ochrona informacji jest na podobnym poziomie abstrakcji, jak fizyka kwantowa. Ich możliwości przyswajania wiedzy z tej dziedziny są mocno ograniczone. Pięciogodzinne szkolenie z zakresu danych osobowych, ISO 27001, informacji niejawnych itp. po prostu ich zmęczy, a efekt niestety będzie daleki od oczekiwań.

Terra incognita czyli bezpieczeństwo informacji u dostawcy

W praktyce bardzo często bywa tak, że organizacja dba o bezpieczeństwo informacji w swoim obrębie, ale nie wymaga tego samego od zewnętrznych dostawców albo podwykonawców usług. Tak oto zewnętrzny dostawca usług IT zarządza kluczowymi systemami IT organizacji w ramach outsourcingu, ale sama organizacja zlecająca nie wie, jaki jest poziom bezpieczeństwa u dostawcy usługi. Czy rzeczywiście jest ono takie, jakiego oczekujemy? Czy powierzone dane rzeczywiście są bezpieczne?

Organizacje nagminnie zapominają o zapewnieniu sobie możliwości kontroli dostawcy, np. poprzez audyty lub odpowiednio szczegółowe raportowanie realizacji usług. Solidni dostawcy nie mają nic do ukrycia i łatwo jest wynegocjować możliwość zastosowania odpowiednich narzędzi oceny ich usługi. Czasami można usłyszeć (jako argument obrony): „nie monitorujemy działań dostawców, ale jakby co, obciążymy ich karami umownymi". Niestety zapomina się o tym, że dostawca nie pójdzie za nas do sądu, jak również nie będzie w naszym imieniu przepraszał klientów. Winowajca zapłaci karę umowną po latach prawnej szarpaniny w sądzie.

Celem niniejszego artykułu było wskazanie błędów popełnianych przez organizacje podczas wdrażania zasad bezpieczeństwa informacji. Mają one specyficzny charakter i często umykają uwadze. Niektóre mogą się wydawać niezbyt poważne, ale praktyka audytowa autora pokazuje, że są one główną przyczyną bardzo poważnych słabości systemu ochrony informacji. Równocześnie, co warto podkreślić, większość z nich da się szybko i tanio usunąć, wystarczy je tylko dostrzec…

Krzysztof Sierota
TÜV Nord Polska

Najnowsze zmiany w prawie zamówień publicznych

Jan Rybczyński

W dniu 22 grudnia 2009 roku weszła w życie tzw. mała nowelizacja ustawy z dnia 29 stycznia 2004 r. *Prawo zamówień publicznych* (Dz.U. z 2007 r. Nr 223, poz. 1655 z późn. zm.) – dalej pzp. Trochę później, w dniu 29 stycznia 2010 r., zaczęła obowiązywać ustawa z 2 grudnia 2009 r. o zmianie ustawy *Prawo zamówień publicznych* oraz niektórych innych ustaw, tzw. duża nowelizacja. Przedsiębiorcy branży ochrony muszą więc poznać w dość krótkim czasie dziesiątki nowych przepisów niełatwej ustawy. Można powiedzieć, że zmiany w zakresie środków ochrony prawnej są najważniejszymi zmianami wprowadzonymi w bieżącym roku. Od tej nowelizacji zacznijmy

Wprowadzenie definicji postępowania o zamówienie publiczne

Przepis art. 2 pkt 7a ustala, że jest to postępowanie wszczynane poprzez publiczne ogłoszenie o zamówieniu lub przesłanie zaproszenia do składania ofert albo do negocjacji w celu dokonania wyboru oferty wykonawcy, z którym zostanie zawarta umowa w sprawie zamówienia publicznego, lub – w przypadku trybu zamówienia z wolnej ręki – wynegocjowania postanowień takiej umowy. Dotychczas, mimo posługiwania się w tym wyrażeniem w przepisach prawa, nie było ono zdefiniowane. Z definicji wynikają ramy czasowe postępowania. Definicja obejmie wszystkie sposoby wszczęcia postępowania, zarówno w trybach konkurencyjnych, jak i niekonkurencyjnych. Za moment wszczęcia postępowania w trybach konkurencyjnych przyjęto zamieszczenie ogłoszenia o zamówieniu. W trybie zapytania o cenę jest to przesłanie zaproszenia do składania ofert, w trybie z wolnej ręki – przesłanie zaproszenia do negocjacji. Według definicji celem postępowania jest wybór oferty wykonawcy, z którym zostanie zawarta umowa w sprawie zamówienia publicznego, lub – w przypadku trybu z wolnej ręki – opracowanie ostatecznej wersji umowy. Z tego wynika moment końcowy postępowania. Końcem postępowania jest decyzja zamawiającego o wyborze najkorzystniejszej oferty lub – w przypadku zamówienia z wolnej ręki – wynegocjowanie postanowień umowy. Wyznaczenie momentu początkowego i końcowego postępowania ma znaczenie z uwagi na określenie zakresu zaskarżenia środkami ochrony prawnej (art. 180 ust. 1). Wykonawcy przysługuje bowiem możliwość wniesienia odwołania na czynności zamawiającego w postępowaniu o udzielenie zamówienia publicznego, czyli na czynności w okresie, który określa definicja.

Wprowadzenie definicji usług

Celem jest zdefiniowanie usług w prawie zamówień publicznych zgodnie z ich definicją zawartą w Dyrektywie 2004/18/WE (tzw. dyrektywie klasycznej). Przez usługi należy rozumieć wszystkie świadczenia, których przedmiotem nie są roboty budowlane lub dostawy i które są usługami określonymi w przepisach wydanych na podstawie art. 2a pzp. Definicja usług odsyła do rozporządzenia Prezesa Rady Ministrów, które zostanie wydane na podstawie ww. przepisu. Wymieniające usługi załączniki do rozporządzenia będą tożsame z załącznikami Dyrektywy. Rozwiązanie to jest zgodne z zasadą odsyłania do innych ustaw albo rozporządzeń prawa wewnętrznego, a nie do aktów prawa unijnego, które, w tym przypadku, jako nie wynikające z dyrektywy, nie są stosowane wprost.

Modyfikacja wśród podmiotów zobowiązanych do stosowania pzp

Uchyleniu ulega art. 3 ust. 1 pkt 6, który przewidywał, że ustawę muszą stosować podmioty, które finansują zamówienie z udziałem środków, których przyznanie było uzależnione od zastosowania procedury przewidzianej w pzp. Również do art. 3 dodany został ust. 3, zgodnie z którym podmioty, przyznając środki finansowe na dofinansowanie projektu, mogą uzależnić ich przyznanie od ich wydatkowania zgodnie z zasadą równego traktowania, uczciwej konkurencji i przejrzystości. Ma to sprawić, by zamówienia były nadal konkurencyjne i ubiegający się o nie wykonawcy byli równo traktowani.

Zmiany w wyłączeniach przedmiotowych

W przepisie art. 4 zmieniono przepis znoszący obowiązek stosowania ustawy w przypadku usług w zakresie badań naukowych i prac rozwojowych oraz świadczenia usług badawczych. Dotychczas musiały być spełnione jednocześnie obie przesłanki, o których mowa niżej, aby wskazane usługi mogły być wyłączone spod reżimu pzp. Zgodnie z pierwszą nie mogły być one w całości opłacane przez zamawiającego, a zgodnie z drugą – ich rezultaty nie mogły stanowić wyłącznej własności zamawiającego. Obecnie do wyłączenia ww. usług wystarczy spełnianie tylko jednej przesłanki.

Drugie wyłączenie polega na dodaniu Internetu do usług związanych z nabyciem, przygotowaniem, produkcją lub koprodukcją materiałów programowych przeznaczonych do emisji w radiu lub telewizji. Jest to zrozumiałe ze względu na rozwój tego środka medialnego.

Krótsze terminy

Skrócono minimalne terminy składania ofert. Dotyczy to przetargu nieograniczonego (art. 43) i ograniczonego (art. 52). W przypadku przetargu ograniczonego, przy zamówieniach o wartości przekraczającej progi unijne, zamawiający będzie mógł wyznaczyć termin składania ofert nie krótszy niż 22 dni, jeżeli zawrze informację o zamówieniu we wstępnym ogłoszeniu informacyjnym i będzie ono zawierać wszystkie wymagane informacje w zakresie, w jakim są one dostępne w momencie publikacji ogłoszenia, a dodatkowo ogłoszenie to zostanie wysłane do Urzędu Oficjalnych Publikacji Wspólnot Europejskich (UOPWE) w celu opublikowania lub zamieszczone w profilu nabywcy na co najmniej 52 dni i nie więcej niż 12 miesięcy przed datą wysłania ogłoszenia o zamówieniu.

W przypadku składania ofert w przetargu nieograniczonym są to następujące terminy.

Zamówienia o wartości poniżej progów unijnych na:

– dostawy lub usługi – termin nie może być krótszy niż 7 dni od dnia zamieszczenia ogłoszenia o zamówieniu w Biuletynie Zamówień Publicznych, dalej BZP (termin bez zmian),
– roboty budowlane – termin nie może być krótszy niż 14 dni od dnia zamieszczenia ogłoszenia o zamówieniu w BZP (wcześniej 20 dni – termin krótszy o 6 dni).

Zamówienia o wartości powyżej progów unijnych na dostawy, usługi, roboty budowlane. Termin nie może być krótszy niż:

– 40 dni od dnia przekazania ogłoszenia o zamówieniu UOPWE drogą elektroniczną zgodnie z formą i procedurami wskazanymi na stronie internetowej określonej w dyrektywie (termin bez zmian),
– 47 dni od dnia przekazania ogłoszenia o zamówieniu UOPWE w inny sposób (termin bez zmian).

Jeżeli informację o zamówieniu (dot. dostaw, usług i robót budowlanych) zawarto we wstępnym ogłoszeniu informacyjnym i zawierało ono wszystkie wymagane informacje w zakresie, w jakim były one dostępne w momencie publikacji ogłoszenia, a ponadto ogłoszenie to zostało wysłane do publikacji w UOPWE lub zamieszczone w profilu nabywcy na co najmniej 52 dni i nie więcej niż 12 miesięcy przed datą wysłania ogłoszenia o zamówieniu, to termin składania ofert wynosi co najmniej:

– 22 dni od dnia przekazania ogłoszenia o zamówieniu UOPWE drogą elektroniczną, zgodnie z formą i procedurami wskazanymi na stronie internetowej określonej w dyrektywie (wcześniej 29 dni – termin krótszy o 7 dni),
– 29 dni od dnia przekazania ogłoszenia o zamówieniu UOPWE w inny sposób (wcześniej 36 dni – termin krótszy o 7 dni).

Ogłoszenie *ex ante*

Wprowadzono nowy typ ogłoszenia – ogłoszenie *ex ante* (art. 62 ust. 2a i 66 ust. 2). Dotyczy to wyłącznie trybów negocjacji bez ogłoszenia oraz z wolnej ręki, w których nie ma ogłoszenia o zamówieniu. Ogłoszenie *ex ante* to ogłoszenie o zamiarze zawarcia umowy w sprawie zamówienia publicznego, które zamawiający może zamieścić w różnych terminach w zależności od trybu udzielenia zamówienia. W przypadku negocjacji bez ogłoszenia zamawiający może zamieścić ogłoszenie po wyborze najkorzystniejszej oferty. W trybie zamówienia z wolnej ręki – po wszczęciu postępowania, czyli po zaproszeniu jedynego wykonawcy do negocjacji. Zamieszczenie takiego ogłoszenia chroni zamawiającego przed zawarciem umowy podlegającej unieważnieniu oraz skraca czas, w jakim potencjalni wykonawcy będą uprawnieni do kwestionowania wyboru trybu, chociaż publikacja ogłoszenia *ex ante* pozwala uzyskać informacje o zamówieniach udzielanych w trybach, w których nie ma obowiązkowego ogłoszenia o zamówieniu, co z kolei umożliwia ewentualne zakwestionowanie wyboru trybu.

Zmiana przesłanek unieważnienia postępowania

Zmieniły się niektóre przesłanki unieważnienia postępowania o zamówienie publiczne. Jeżeli zamawiający zwiększy kwotę przeznaczoną na sfinansowanie zamówienia do ceny najkorzystniejszej oferty, to nie będzie musiał unieważnić postępowania (art. 93 ust. 1 pkt 4 i 7). Zatem obecnie zamawiający będzie unieważniał postępowania, jeżeli cena najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba że zamawiający zwiększy tę kwotę do ceny najkorzystniejszej oferty. Dodano nową przesłankę unieważnienia postępowania (art. 93 ust. 1b) dotyczącą przypadku nieprzyznania zamawiającemu środków unijnych lub od państw członkowskich EFTA. Warunkiem jest przewidzenie takiej możliwości odpowiednio – w zależności od trybu – w ogłoszeniu o zamówieniu, zaproszeniu do negocjacji lub zaproszeniu do składania ofert.

Zawieszenie umowy

W przepisie art. 94 wprowadzono termin *standstill*, tj. termin zawieszenia możliwości zawarcia umowy w sprawie zamówienia publicznego. Terminem tym posługuje się dyrektywa 2007/66/WE Parlamentu Europejskiego i Rady z 11 grudnia 2007 r. zmieniająca dyrektywę Rady 89/665/EWG i 92/13/EWG w zakresie poprawy skuteczności procedur odwoławczych w dziedzinie udzielania zamówień publicznych, zwana dyrektywą odwoławczą. Wprowadzenie tego terminu ma zapewnić większą efektywność środków ochrony prawnej wnoszonych przez wykonawców. Termin zawieszenia możliwości zawarcia umowy jest liczony od dnia przesłania wykonawcom informacji o wyborze najkorzystniejszej oferty. Zależy on od wartości zamówienia oraz sposobu poinformowania wykonawcy przez zamawiającego o wyborze najkorzystniejszej oferty. W przypadku zamówień o wartości przekraczającej progi unijne jest to 10 lub 15 dni. Termin wynosi 10 dni, gdy zamawiający poinformuje wykonawców w formie elektronicznej lub faksem. Zamawiający będzie mógł więc zawrzeć umowę po upływie 10 dnia. Jeżeli zamawiający poinformuje wykonawców w inny sposób, będzie mógł zawrzeć umowę dopiero po 15 dniach. W przypadku zamówień podprogowych terminy te wynoszą odpowiednio, w zależności od sposobu poinformowania wykonawcy, 5 lub 10 dni. Naruszenie terminu *standstill* daje Krajowej Izbie Odwoławczej (KIO) uprawnienie do nałożenia na zamawiającego kary finansowej w wysokości do 5 proc. wartości wynagrodzenia wykonawcy przewidzianego w umowie. Przewidziano jednakże pięć wyjątków od zasady *standstill* (art. 94 ust. 2). Oto one:

1) Zamawiający może zawrzeć umowę w sprawie zamówienia przed upływem ustawowych terminów, jeśli w przetargu nieograniczonym złożono tylko jedną ofertę. Dotyczy to przetargu ograniczonego, negocjacji z ogłoszeniem i dialogu konkurencyjnego, gdy złożono tylko jedną ofertę, a w sytuacji wykluczenia wykonawcy upłynął termin wniesienia odwołania lub w następstwie jego wniesienia KIO ogłosiła wyrok lub postanowienie kończące postępowanie odwoławcze.
2) Umowa odnosi się do zamówienia udzielanego w trybie negocjacji bez ogłoszenia, w ramach dynamicznego systemu zakupów albo na podstawie umowy ramowej.
3) Gdy w postępowaniu o wartości niższej niż progi unijne nie odrzucono żadnej oferty oraz gdy w przetargu nieograniczonym albo zapytaniu o cenę nie wykluczono żadnego wykonawcy; także wtedy, gdy w przypadku trybu przetargu ograniczonego, negocjacji z ogłoszeniem, dialogu konkurencyjnego i licytacji elektronicznej upłynął termin wniesienia odwołania na czynność wykluczenia wykonawcy lub w następstwie jego wniesienia KIO ogłosiła wyrok lub postanowienie kończące postępowanie odwoławcze.
4) Postępowanie jest prowadzone w trybie licytacji elektronicznej (z wyjątkiem przypadku wykluczenia wykonawcy, wobec którego nie upłynął jeszcze termin wniesienia odwołania lub w następstwie jego wniesienia KIO nie ogłosiła jeszcze wyroku lub postanowienia kończącego postępowanie odwoławcze).
5) Wykonawca, którego ofertę wybrano, uchyla się od zawarcia umowy lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy. W tym przypadku zamawiający może wybrać kolejną najkorzystniejszą ofertę spośród pozostałych ofert – nie tylko bez przeprowadzania ich ponownej oceny, ale i badania, chyba że zachodzą przesłanki unieważnienia postępowania. Jeśli drugi wykonawca też uchyli się od zawarcia umowy, zamawiający analogicznie wybiera kolejnego (też bez ponownego badania i oceny), aż do skutku, przy czym już po wyborze drugiego wykonawcy zamawiający musi zachować termin *standstill*.

Nowe przesłanki unieważnienia umowy

Przepis art. 146 zawiera trzy nowe przesłanki unieważnienia umowy. Umowa jest unieważniana, jeżeli zamawiający:

– z naruszeniem przepisów ustawy zastosował tryb negocjacji bez ogłoszenia lub zamówienia z wolnej ręki;
– nie zamieścił ogłoszenia o zamówieniu w BZP albo nie przekazał ogłoszenia o zamówieniu Urzędowi Oficjalnych Publikacji Wspólnot Europejskich;
– zawarł umowę z naruszeniem wskazanych przepisów pzp (art. 94 ust. 1 lub art. 183 ust. 1), jeśli uniemożliwiło to KIO uwzględnienie odwołania przed zawarciem umowy;
– uniemożliwił składanie ofert orientacyjnych wykonawcom niedopuszczonym dotychczas do udziału w dynamicznym systemie zakupów lub uniemożliwił wykonawcom dopuszczonym do udziału w dynamicznym systemie zakupów złożenie ofert w postępowaniu o udzielenie zamówienia prowadzonym w ramach tego systemu;
– udzielił zamówienia na podstawie umowy ramowej przed upływem warunków wskazanych w pzp;
– zastosował tryb zapytania o cenę z naruszeniem przepisów ustawy.

Nie ma protestów

Jak wspomniałem na początku, czas na przedstawienie jednej z najważniejszych zmian i jej skutków. W nowelizacji grudniowej nastąpiła całkowita rezygnacja z instytucji protestu. Odwołanie będzie wnoszone do Prezesa KIO (art. 180 ust. 4), a nie, jak dotychczas, do Prezesa Urzędu Zamówień Publicznych. Dopuszczono nową formę wnoszenia odwołania – elektroniczną, opatrzoną bezpiecznym podpisem elektronicznym. Wykonawca jest teraz zobowiązany przesłać kopię odwołania zamawiającemu przed upływem terminu do jego wniesienia w taki sposób, aby zamawiający mógł zapoznać się z jego treścią przed upływem tego terminu. Niezwłocznie, nie później niż w terminie dwóch dni od dnia otrzymania, zamawiający będzie przesyłał kopię odwołania innym uczestnikom postępowania w celu umożliwienia im przystąpienia do postępowania odwoławczego. Wykonawcy będą mogli przystąpić do postępowania odwoławczego w terminie trzech dni od otrzymania kopii odwołania od zamawiającego.

Czas na wniesienie odwołania (art. 182) uregulowano w zależności od wartości zamówienia oraz sposobu przesyłania przez zamawiającego informacji stanowiącej podstawę wniesienia odwołania. Terminy to odpowiednio 10 i 15 dni w przypadku zamówień o wartości przekraczającej progi europejskie oraz 5 i 10 dni w przypadku zamówień podprogowych (terminy są krótsze w przypadku przesłania przez zamawiającego informacji stanowiącej podstawę do wniesienia odwołania faksem lub drogą elektroniczną, dłuższe, jeżeli przesłano ją w inny sposób).

Przy zamówieniach o wartości przekraczającej progi europejskie odwołanie wobec treści ogłoszenia o zamówieniu oraz w przetargu nieograniczonym również wobec treści specyfikacji istotnych warunków zamówienia wykonawca składa się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej (Dz. U. UE) lub zamieszczenia specyfikacji istotnych warunków zamówienia na stronie internetowej. Przy zamówieniach podprogowych odwołanie musi być złożone w ciągu pięciu dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych (BZP) lub specyfikacji istotnych warunków zamówienia na stronie internetowej. Czas na wniesienie odwołania wobec innych czynności to 10 dni od dnia, w którym powzięto lub – przy zachowaniu należytej staranności – można było powziąć wiadomość o okolicznościach stanowiących podstawę do wniesienia odwołania w przypadku zamówień o wartości przekraczającej progi unijne, oraz pięć dni w przypadku zamówień, których wartość nie przekracza tych progów.

Jeżeli zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy, nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty (mimo że jest to obowiązkowe) lub nie zaprosił go do złożenia oferty w ramach dynamicznego systemu zakupów bądź umowy ramowej, odwołanie będzie wnoszone nie później niż w terminie:

– 15 dni od dnia zamieszczenia ogłoszenia o udzieleniu zamówienia w BZP albo 30 dni od dnia opublikowania go w Dz.U. UE,
– 6 miesięcy od dnia zawarcia umowy, jeżeli zamawiający nie opublikował ogłoszenia o udzieleniu zamówienia w Dz.U. UE lub opublikował je w trybach negocjacji bez ogłoszenia i z wolnej ręki bez uzasadnienia,
– 1 miesiąca od dnia zawarcia umowy, jeżeli zamawiający nie zamieścił ogłoszenia o udzieleniu zamówienia w BZP albo zamieścił je w trybach negocjacji bez ogłoszenia, zamówienia z wolnej ręki lub zapytania o cenę bez uzasadnienia.

Szybkie ale i kosztowne rozpatrywanie odwołań

Jak wiemy, zlikwidowano bezpłatne protesty. Odwołania będą rozpatrywane w składach jednoosobowych (trzech arbitrów będzie rozpatrywać tylko sprawy szczególnie zawiłe lub o precedensowym charakterze), z zasady na posiedzeniu niejawnym. KIO może jednak wezwać strony lub biegłych do udziału w takim posiedzeniu. W przypadku odrzucenia odwołania lub umorzenia postępowania odwoławczego Krajowa Izba Odwoławcza nie będzie miała obowiązku ogłaszania postanowienia. Odwołanie zostanie uwzględnione, jeżeli KIO stwierdzi naruszenie przepisów ustawy, które miało wpływ lub mogło mieć istotny wpływ na wynik postępowania.

Wprowadzono zakaz zawarcia umowy do czasu ogłoszenia przez KIO wyroku lub postanowienia kończącego postępowanie odwoławcze. Zakaz ten jest możliwy do uchylenia przez KIO w przypadku, gdy niezawarcie umowy mogłoby spowodować szkody dla interesu publicznego, przewyższające korzyści związane z ochroną wszystkich partykularnych interesów, które mogą doznać uszczerbku w wyniku czynności podjętych przez zamawiającego w postępowaniu. Izba rozpoznaje odwołanie w terminie 15 dni od dnia jego doręczenia Prezesowi Izby. Według zmienionego w ubiegłym roku rozporządzenia Prezesa Rady Ministrów z dnia 9 lipca 2007 r. w sprawie wysokości oraz sposobu pobierania wpisu od odwołania oraz rodzajów kosztów w postępowaniu odwoławczym i sposobu ich rozliczania wpis od odwołania dot. usług i dostaw o wartości poniżej progów unijnych kosztuje 7,5 tys. złotych, a wpis o równej lub wyższej od tego progu wartości – dwukrotność tej kwoty. O opłatach sądowych od skarg na orzeczenia KIO można powiedzieć, że są horrendalnie wysokie.

Skarga wnoszona do sądu okręgowego na orzeczenia KIO pełni rolę apelacji. Opłata sądowa od skargi wynosi pięciokrotność

wpisu od odwołania wniesionego w sprawie, której dotyczy skarga. W przypadku skargi dotyczącej czynności zamawiającego dokonanej po otwarciu ofert (np. wyboru oferty) opłata ta wynosi 5% wartości przedmiotu zamówienia, nie więcej niż 5 mln zł. Zatem teraz, w celu zakwestionowania działań zamawiającego, wykonawca będzie musiał od razu wnieść odwołanie do KIO i ponieść związane z tym koszty wpisu, a potem, ewentualnie, opłaty sądowej. Dotyczy to również zamawiającego. W przetargach podprogowych na większość czynności zamawiającego wykonawcom nie przysługuje żaden środek ochrony prawnej. Istnieje jedynie prawo poinformowania zamawiającego o tym, że postąpił niezgodnie z prawem. Jeżeli toczy się postępowanie odwoławcze, zamawiający może uwzględnić wszystkie zarzuty odwołania. W takim przypadku KIO umorzy postępowanie odwoławcze, jeżeli zgodzą się na to wszyscy wykonawcy, którzy przystąpili do postępowania odwoławczego po stronie zamawiającego.

Nowa instytucja opozycji i odpowiedzi zamawiającego

Należy wspomnieć, że wprowadzono też nową instytucję – instytucję opozycji. Zamawiającemu i wykonawcy przysługuje prawo zgłoszenia opozycji przeciw przystąpieniu innego wykonawcy do postępowania odwoławczego. Opozycję można zgłosić nie później niż do czasu otwarcia rozprawy. KIO nie zbada z urzędu, czy wykonawca przystępujący do postępowania odwoławczego ma w tym interes. To strona zgłaszająca opozycję będzie musiała wykazać, że takiego interesu on nie ma. Dopiero wtedy KIO będzie mogła uwzględnić opozycję i nie dopuścić wykonawcy do uczestnictwa w postępowaniu odwoławczym.

Po zmianach zamawiający dysponuje prawem do odpowiedzi na odwołanie (art. 186 ust. 1), w tym do jego uwzględnienia. Jeśli zamawiający uwzględni zarzuty zawarte w odwołaniu w całości przed posiedzeniem, to KIO może umorzyć postępowanie na posiedzeniu niejawnym bez udziału stron. Umorzenie postępowania nastąpi też wtedy, gdy wykonawca przystąpi do postępowania odwoławczego po stronie zamawiającego i nie wniesie sprzeciwu wobec uwzględnienia przez zamawiającego w całości zarzutów z odwołania (art. 186 ust. 3). Jeśli natomiast wykonawca, który przystąpił do postępowania odwoławczego po stronie zamawiającego, sprzeciwi się uwzględnieniu zarzutów z odwołania w całości (pisemnie lub ustnie do protokołu), wtedy KIO rozpozna sprawę merytorycznie.

Ważniejsze zmiany obowiązujące od 22 grudnia 2009 r.

Jak stwierdzono na początku, wiele zmian wprowadziła również ustawa z 5 listopada 2009 r. o zmianie ustawy *Prawo zamówień publicznych oraz ustawy o kosztach sądowych w sprawach cywilnych*, która weszła w życie 22 grudnia 2009 r.

Terminy wyjaśnień do SIWZ

Zgodnie ze zmienionym art. 38 wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, nie później niż:

– sześć dni przed upływem terminu składania ofert,
– cztery dni przed upływem terminu składania ofert – w przetargu ograniczonym oraz w negocjacjach z ogłoszeniem, jeśli zachodzi pilna potrzeba udzielenia zamówienia,
– dwa dni przed upływem terminu składania ofert w przypadku zamówień o wartości poniżej progów unijnych, o ile wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął do zamawiającego nie później niż do końca dnia, w którym upływa połowa terminu składania ofert.

Zakres zabezpieczenia

Nastąpiło zawężenie zakresu zabezpieczenia tylko do roszczeń z tytułu niewykonania lub nienależytego wykonania umowy, w tym roszczeń z tytułu rękojmi za wady. Dla wykonawców oznacza to, że nie będą musieli zamrażać środków finansowych przez często długi okres trwania gwarancji, zastrzeżony w umowie w sprawie zamówienia publicznego. Nowela z dnia 5 listopada 2009 r. nie dokonała zmian formy, wysokości i momentu wniesienia zabezpieczenia.

Warunki udziału w postępowaniu

Warunki pozytywne i negatywne wyodrębniono w dwóch różnych artykułach.

Doprecyzowano przepisy dotyczące momentu, w którym wykonawca potwierdza spełnianie warunków udziału w postępowaniu. Momentem tym jest dzień składania ofert. Ponadto nowe rozwiązania wprowadziły uelastycznienie sposobu potwierdzania spełniania tych warunków. Obecnie wykonawcy mogą się powoływać np. na doświadczenie i potencjał techniczny podmiotów trzecich. Ciężar wykazania spełniania warunków udziału w postępowaniu spoczywa zawsze na wykonawcy. Zatem zgodnie z nowym przepisem art. 26 ust. 2b wykonawca może polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia oraz zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków.

Warto tę kwestię trochę rozwinąć, gdyż firmy ochrony świadczą część usług w ramach tzw. zarządzania nieruchomościami lub wykonywania koncesjonowanej części umów związanych z wykonaniem zabezpieczenia technicznego.

W takiej sytuacji wykonawca (może to być firma ochrony, ale nie musi) jest zobowiązany jedynie do udowodnienia zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia.

Zmiana ta ma istotne znaczenie praktyczne. Dotychczas nie było możliwości skorzystania z doświadczenia osób trzecich. Gdy wykonawca nie był w stanie wykazać się wymaganymi przez zamawiającego wszystkimi „właściwościami", wyjściem było utworzenie konsorcjum. Wszyscy członkowie konsorcjum solidarnie odpowiadali przed zamawiającym. Zmiany umożliwiają współpracę kilku podmiotów niezależnie od łączących je stosunków, tj. bez konieczności utworzenia konsorcjum. Wykonawca będzie uprawniony do wykazania doświadczenia poprzez samo przedstawienie oświadczeń podmiotów, z którymi będzie współpracować podczas wykonywania zamówienia. W rezultacie tylko jeden podmiot będzie odpowiadać przed

zamawiającym. Pozostali przekażą mu odpowiedni potencjał, zgodnie ze złożonymi wcześniej oświadczeniami. Z pewności nastąpi oderwanie potencjału firmy od jej uprawnień wynikających z decyzji administracyjnych, np. decyzji koncesyjnej.

Zabezpieczenie umowy

Zrezygnowano z żądania obligatoryjnego zabezpieczenia należytego wykonania umowy. Obecnie zabezpieczenie jest fakultatywne. Zmniejszy to koszty ponoszone przez wykonawców.

Wadium

Obecnie zamawiający zwraca wadium wszystkim wykonawcom z wyjątkiem wykonawcy, którego ofertę wybrał jako najkorzystniejszą, niezwłocznie po wyborze najkorzystniejszej oferty lub po unieważnieniu postępowania (nie z chwilą podpisania umowy, jak dotychczas). Wpłynie to korzystnie na płynność finansową wykonawców. Również wtedy, gdy wykonawca wycofa ofertę przed upływem terminu składania ofert, zamawiający musi zwrócić mu wadium niezwłocznie. Obowiązek żądania przez zamawiającego ponownego wniesienia wadium przez wykonawcę, któremu wadium już zwrócono, dotyczy obecnie tylko tego wykonawcy, którego ofertę wybrano jako najkorzystniejszą w wyniku ostatecznego rozstrzygnięcia KIO.

Zaliczki

Wprost do ustawy wprowadzono uprawnienie zamawiającego do udzielania zaliczek na poczet wynagrodzenia wykonawcy. Zamawiający z podsektora rządowego mogą udzielać zaliczek w przypadku zamówień na roboty budowlane lub na wszystkie kategorie zamówień (roboty budowlane, usługi, dostawy), gdy są one finansowane ze środków państw członkowskich UE i EFTA lub innych środków zagranicznych nie podlegających zwrotowi. Ograniczenie nie dotyczy jednostek samorządu terytorialnego i ich związków oraz innych jednostek sektora finansów publicznych, których organem założycielskim lub nadzorującym jest jednostka samorządu terytorialnego. Samorządy mogą zatem udzielać zaliczek na wszystkie kategorie zamówień niezależnie od źródeł finansowania zamówienia. Równocześnie zamawiający zostali zobligowani do żądania zabezpieczenia udzielonej zaliczki w przypadku, gdy jej wartość przekracza 20 proc. wynagrodzenia wykonawcy przewidzianego w umowie. Wykonawca wnosi zabezpieczenie w takich formach, w jakich zabezpiecza należyte wykonanie umowy.

Ostatnia, ale nie mniej ważna dla branży ochrony zmiana

W przepisie art. 22 ust. 2 wdrożono postanowienie tzw. dyrektywy klasycznej, zgodnie z którym zamawiający może zastrzec, że o zamówienia mogą ubiegać się wyłącznie wykonawcy, u których ponad 50 proc. zatrudnionych pracowników stanowią osoby niepełnosprawne (tzw. zamówienia zastrzeżone). Wiadomo, że pewna część firm ochrony ma status zakładów pracy chronionej. By ocenić wpływ tego przepisu na rynek ochrony, trzeba trochę poczekać.

mecenas Jan Rybczyński
radca prawny

Art. opracowany na podstawie tekstu zamieszczonego w Biuletynie Informacyjnym Nr 1/2010 Polskiej Izby Ochrony (PIO).

ZARZĄDZANIE BEZPIECZEŃSTWEM OBIEKTÓW

O ZNACZENIU MILITARNYM

Piotr Januszkiewicz

Zarządzanie bezpieczeństwem obiektów o znaczeniu militarnym było, jest i będzie jednym z najważniejszych zadań Sił Zbrojnych Rzeczypospolitej Polskiej. Wzrosło zagrożenie ze strony zorganizowanych grup przestępczych, mających na celu m.in. pozyskiwanie broni, amunicji i materiałów wybuchowych. Jednocześnie rozwinął się terroryzm, a „opłacalnym" celem ataków grup terrorystycznych mogą stać się obiekty wojskowe. Bezpieczeństwo obiektów militarnych można zapewnić między innymi poprzez skuteczną ochronę, która zawsze zależała od możliwości wykrycia obecności intruza – jeszcze przed wejściem do stref szczególnie chronionych – i poinformowania o tym fakcie służb ochrony fizycznej. Rozwój elektroniki, a szczególnie mikroelektroniki i optoelektroniki, spowodował gwałtowny rozwój central alarmowych oraz czujek wykrywających obecność intruzów w chronionych strefach

Z oceny funkcjonowania systemów ochrony obiektów wojskowych wynika, że najsłabszymi ich ogniwami nadal pozostają ludzie, którzy wyznaczani są do ochrony, a także wadliwie skonstruowane systemy bezpieczeństwa.

Z tego powodu w resorcie obrony narodowej opracowano wiele dokumentów normatywnych, w których określono wymagania techniczno-użytkowe dla poszczególnych systemów zabezpieczeń.

Wybrane zagadnienia zarządzania bezpieczeństwem obiektów wojskowych

Zarządzanie bezpieczeństwem obiektów wojskowych jest realizowane przez osoby funkcyjne na podstawie wielu dokumentów normatywnych, do których należy m.in.:

1) Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (**Dz.U. z 2005 r. Nr 145, poz. 1221 z późn. zm.**).
2) Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (**Dz.U. z 2005 r. Nr 196, poz. 1631**).
3) Rozporządzenie Rady Ministrów z dnia 18 grudnia 2001 r. w sprawie użycia środków przymusu bezpośredniego oraz broni palnej przez żołnierzy wojskowych organów porządkowych (**Dz.U. Nr 157, poz. 1838**).
4) Rozporządzenie Rady Ministrów z dnia 30 czerwca 1998 r. w sprawie szczegółowych warunków i sposobu postępowania pracowników ochrony przy użyciu broni palnej. (**Dz.U. Nr 86, poz. 543**).
5) Rozporządzenie Rady Ministrów z dnia 30 czerwca 1998 r. w sprawie szczegółowych warunków i sposobów użycia przez pracowników ochrony środków przymusu bezpośredniego (**Dz.U. Nr 89, poz. 563**).
6) Rozporządzenie Ministra Obrony Narodowej z dnia 2 czerwca 1999 r. w sprawie wewnętrznych służb ochrony działających na terenach komórek i jednostek organizacyjnych resortu obrony narodowej (**Dz.U. Nr 58, poz. 619 z późn. zm.**).
7) Rozporządzenie Ministra Obrony Narodowej z dnia 19 czerwca 1999 r. w sprawie ochrony przez specjalistyczne uzbrojone formacje ochronne terenów komórek i jednostek organizacyjnych resortu obrony narodowej (**Dz.U. Nr 60, poz. 647 z późn. zm.**).
8) Instrukcja o ochronie obiektów wojskowych (**OIN 3/2008**).
9) Regulamin oddziałów wart cywilnych (**OIN 1/2007**).
10) Norma Obronna NO-04-A004:2010 *Obiekty wojskowe. Systemy alarmowe*:
   – arkusz 1 – *Wymagania ogólne*,
   – arkusz 2 – *Wymagania techniczno-użytkowe*,
   – arkusz 3 – *Metody określania liczby urządzeń*,
   – arkusz 4 – *Wymagania dotyczące urządzeń*,
   – arkusz 5 – *Wymagania dotyczące tablicy synoptycznej*,
   – arkusz 6 – *Wymagania dotyczące systemów kontroli dostępu*,
   – arkusz 7 – *Wymagania dotyczące telewizyjnych systemów nadzoru*,
   – arkusz 8 – *Eksploatacja*,

Jednym z elementów systemów bezpieczeństwa obiektów wojskowych jest właściwa ochrona fizyczna i techniczna tych obiektów.

Ochrona obiektów wojskowych to zespół przedsięwzięć, które uniemożliwiają nielegalne przedostanie się osób, pojazdów, statków pływających lub powietrznych oraz wniesienie sprzętu lub materiałów niebezpiecznych na teren chronionych obiektów wojskowych, a także zabezpieczają znajdujące się tam mienie przed kradzieżą, zniszczeniem lub uszkodzeniem.

Osoby odpowiedzialne za organizację skutecznego systemu ochrony obiektu wojskowego podczas prowadzonych systematycznie analiz zagrożeń powinny wziąć pod uwagę zarówno zagrożenia zewnętrzne, jak i wewnętrzne. To na analizie zagrożeń, przedstawionej w odpowiednim dokumencie, powinno być oparte projektowanie właściwego systemu ochrony.

Zagrożenie zewnętrzne dla ochranianych obiektów i mienia wojskowego mogą stanowić:

– zorganizowane grupy przestępcze i terroryści, działający w sposób profesjonalny, przemyślany i zorganizowany, często bezwzględny,
– pojedynczy przestępcy,
– osoby psychicznie niezrównoważone,
– przypadkowe osoby wykorzystujące nadarzającą się okazję, zaistniałą z powodu nieprawidłowego zabezpieczenia i nieprawidłowej ochrony mienia wojskowego,
– grupy młodych ludzi lub pojedyncze osoby młodociane, które chcą zaimponować kolegom,
– byli żołnierze, znający system ochrony i miejsce składowania poszczególnych rodzajów sprzętu i środków bojowych, którzy w cywilu zeszli na drogę przestępczą,
– pobliska ludność, która zamierza nielegalnie pozyskać np. sprzęt i materiały budowlane, siatkę ogrodzeniową, kable, paliwo itp.,
– obywatele państw obcych.

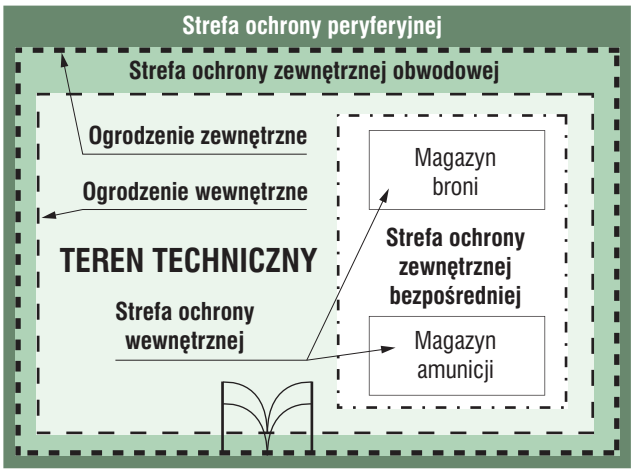
Zagrożenie wewnętrzne dla ochranianych obiektów i mienia wojskowego mogą stanowić:

– magazynierzy, którzy na skutek niegospodarności lub celowych działań spowodowali straty (ubytki) w przechowywanym mieniu i próbują nielegalnie je uzupełnić albo upozorować włamanie,
– osoby zabezpieczające funkcjonowanie jednostki i mające dostęp do magazynów lub miejsc przechowywania mienia wojskowego,
– osoby angażowane do prac porządkowych na terenach technicznych, w magazynach lub innych miejscach przechowywania mienia,
– wartownicy, pracownicy ochrony i osoby pełniące służby dyżurne.

Strefy ochrony w obiekcie wojskowym i funkcje systemu ochrony technicznej

Właściwe zabezpieczenie sprzętu bojowego oraz broni, amunicji i materiałów wybuchowych, jako najważniejszego mienia wojskowego, powinno sprowadzać się do posiadania sprawnie działających sił ochronnych (ochrony fizycznej) oraz kompleksowego zabezpieczenia technicznego (ochrony technicznej), tworzących system ochrony.

Jakie wymagania powinien spełniać system ochrony technicznej? Powinien wykryć każdą próbę niekontrolowanego wejścia (wtargnięcia) na teren chroniony – już w chwili przekroczenia jego granicy. Takie wczesne wykrycie intruza powinno być zapewnione przez system w strefie ochrony zewnętrznej obwodowej. Dojście do strefy wokół poszczególnych obiektów (budynków) na terenie ochranianym powinno



Rys. 1. Strefa ochrony w obiekcie wojskowym

być sygnalizowane przez system w strefie ochrony zewnętrznej bezpośredniej. Natomiast systemy ochrony wewnętrznej powinny sygnalizować przebywanie intruza w budynku, magazynie lub pomieszczeniu.

Uwzględniając powyższe rozróżnienia, należy podzielić chroniony teren obiektu wojskowego na strefy.

Strefa ochrony peryferyjnej – wydzielony obszar terenu poza ogrodzeniem zewnętrznym obiektu wojskowego. W strefie tej nie instaluje się urządzeń i systemów alarmowych, natomiast utrzymuje się pas o szerokości 25 m, wolny od wysokich zarośli, krzewów i traw, umożliwiający wgląd w teren przyległy do chronionego obiektu. Pasa tego nie utrzymuje się w przypadku, gdy strefa ochrony peryferyjnej obejmuje obszar nie będący terenem wojskowym.

Strefa ochrony zewnętrznej obwodowej – obszar terenu znajdujący się pomiędzy zewnętrznym i wewnętrznym ogrodzeniem obiektu wojskowego. W strefie tej instaluje się zewnętrzne urządzenia i systemy alarmowe, oświetlenie, system łączności przewodowej dla sił ochronnych. W strefie ochrony zewnętrznej obwodowej należy stosować co najmniej dwa niezależnie działające systemy alarmowe, np.: system ogrodzeniowy i system powierzchniowy, system ogrodzeniowy i system podziemny, dwa systemy powierzchniowe, w tym aktywne tory podczerwieni i bariery mikrofalowe, oraz inne kombinacje systemów.

W bardzo złych (granicznych) warunkach atmosferycznych minimalny zasięg pracy czujek w strefie ochrony obwodowej nie może być mniejszy niż 60% zasięgu transmisji w warunkach normalnych dla czujek podczerwieni oraz 80% dla czujek mikrofalowych (wymaganie to nie dotyczy systemów wideodetekcji).

Strefa ochrony zewnętrznej bezpośredniej – obszar terenu bezpośrednio przylegający do poszczególnych magazynów, budynków w obiekcie wojskowym. W strefie tej instalowane są zewnętrzne urządzenia i systemy alarmowe, które mogą współpracować z kamerami telewizyjnych systemów nadzoru. W strefie ochrony zewnętrznej bezpośredniej należy stosować pojedyncze systemy alarmowe – naziemne, podziemne lub ogrodzeniowe. Wybierając urządzenia mające wchodzić w skład poszczególnych systemów, należy brać pod uwagę ich zasięgi, które muszą być dostosowane do wielkości ochranianych budynków lub rejonów. Zainstalowane w strefie ochrony zewnętrznej bezpośredniej urządzenia powinny współpracować z telewizyjnymi systemami nadzoru i weryfikować zdarzenia alarmowe.

Strefa ochrony wewnętrznej – obszar wewnątrz magazynów, budynków wraz ze wszystkimi otworami okiennymi, drzwiowymi, wywietrznikami itp. W strefie tej instaluje się wewnętrzne urządzenia i systemy alarmowe. Można wykorzystywać w niej także kamery telewizyjnych systemów nadzoru współpracujące z wewnętrznymi urządzeniami alarmowymi oraz inne urządzenia wspomagające ochronę fizyczną tej strefy. W strefie ochrony wewnętrznej, szczególnie w magazynach uzbrojenia, instaluje się systemy alarmowe z co najmniej dwoma rodzajami czujek, które działają na odmiennych zasadach (np. czujki podczerwieni i mikrofalowe lub podczerwieni i ultradźwiękowe).

W magazynach, w których przechowuje się broń strzelecką, należy dodatkowo zainstalować czujki zbicia szkła, jeżeli w oknach tych magazynów zamontowane są zwykłe szyby.

Zainstalowane urządzenia alarmowe powinny obejmować swoim zasięgiem całe pomieszczenia magazynowe. W tych pomieszczeniach nie może być tzw. martwych pól, w których obecność intruza nie jest wykrywalna. W magazynach broni oraz innych pomieszczeniach podlegających szczególnej ochronie nie należy instalować czujek dualnych.

Zmiany aktualizacyjne w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe omówiono w odrębnym artykule – patrz s. 76 *Zabezpieczeń*.

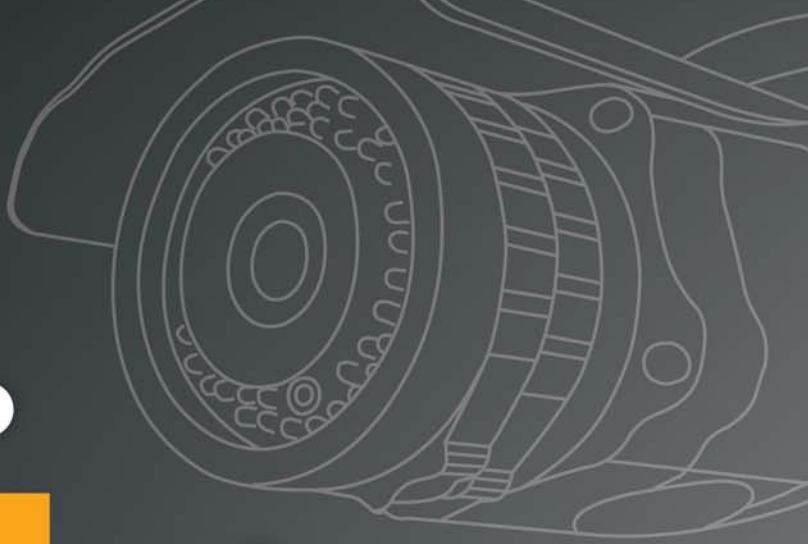
mgr inż. Piotr Januszkiewicz

System ochrony technicznej musi spełniać następujące funkcje:	
wczesne wykrycie wtargnięcia	Każda próba wtargnięcia musi być wykryta przez urządzenia elektroniczne znajdujące się w strefie zewnętrznej lub – w przypadku jej braku – wewnętrznej.
rozpoznanie źródła alarmu	Każdy wywołany w systemie alarm musi być rozpoznany pod względem źródła, które go wywołało (np. alarm techniczny – niesprawność czujki, alarm właściwy – intruz).
opóźnienie działania intruza	Ewentualny intruz musi napotkać na swej drodze bariery mechaniczne w postaci ogrodzeń, metalowych lub obitych blachą drzwi, krat, szyb zabezpieczonych folią antywłamaniową, kłódek, atestowanych zamków wewnętrznych itp., które wydłużą czas jego dotarcia do obiektu, aby umożliwić skuteczne przeciwdziałanie.
właściwa komunikacja	Każda informacja pochodząca z urządzenia alarmowego, czujki, przycisku napadowego, kamery itp., musi dotrzeć do właściwego centrum nadzoru systemu i uruchomić te siły i środki, które są niezbędne do przeciwdziałania zagrożeniu.
przeciwdziałanie	Każdy rozpoznany alarm powinien spowodować podjęcie odpowiednich działań interwencyjnych przez właściwe siły ochronne

Tab. 1. Zadania systemu ochrony technicznej

4 POZIOMY BEZPIECZEŃSTWA

Nowe serie kamer marki NOVUS®



seria G

- Czułość od 0.00003 lx
- Do 600 TVL w kolorze
- DSS (wydłużona migawka)
- OSD w języku polskim (menu ekranowe)
- Sterowanie RS-485 (oprócz kamer kopułkowych)
- WDR (szeroki zakres dynamiki)
- HLC (redukcja oślepiania)
- Strefy prywatności
- Zoom cyfrowy
- Detekcja ruchu
- DIS (cyfrowa stabilizacja obrazu)
- Oświetlacz podczerwieni (kamery wandaloodporne)
- Obiektyw f=2.5~12 mm (oprócz kamer kompaktowych)

seria H

- Czułość od 0.00004 lx
- Do 560 TVL w kolorze
- DSS (wydłużona migawka)
- OSD (menu ekranowe)
- WDR (szeroki zakres dynamiki)
- HLC (redukcja oślepiania)
- Strefy prywatności
- Zoom cyfrowy
- Detekcja ruchu

seria B

- Czułość od 0.01 lx
- Do 600 TVL w kolorze
- OSD (menu ekranowe)
- Sterowanie RS-485 (kamery kompaktowe)
- Strefy prywatności
- Detekcja ruchu
- Obiektyw f=2.8~10.5 mm (oprócz kamer kompaktowych)

seria E

- Czułość od 0.05 lx (0 lx przy włączonym oświetlaczu IR)
- Do 540 TVL w kolorze
- Oświetlacz podczerwieni

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

System bezpieczeństwa obiektu dydaktycznego

Termin „obiekt dydaktyczny” oznacza wszelkiego rodzaju szkoły podstawowe, gimnazja, licea, wyższe uczelnie i placówki naukowe. W niniejszym artykule przeanalizujemy zagadnienia bezpieczeństwa i zabezpieczeń w szkole średniej

Adam Rudzki

W szkole uczą się zarówno osoby niepełnoletnie, jak i dorosłe. Przekrój wiekowy i społeczny osób, które uczęszczają do szkoły, jest bardzo duży. Szkoła jest z pozoru miejscem bezpiecznym, jednak statystyki policyjne dowodzą, że jest inaczej. Codzienna rzeczywistość wielu liceów, gimnazjów, a nawet szkół podstawowych to kradzieże, włamania, rozboje, pobicia i narkotyki. Statystyki policyjne z ubiegłych lat pokazują skalę zdarzenia [1].

Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz.U. z 2003 r. nr 6, poz. 69) nakłada na dyrektora szkoły lub placówki obowiązek zapewnienia bezpiecznych i higienicznych warunków nauki i pracy w szkole i na jej terenie.

System bezpieczeństwa szkoły można podzielić na trzy części:
– rozwiązania organizacyjne,
– przedsięwzięcia profilaktyczno-wychowawcze,
– zabezpieczenia techniczne.

Zabezpieczenia techniczne szkół możemy podzielić na:
– systemy sygnalizacji włamania i napadu (SSWiN),
– system nadzoru wizyjnego,
– system sygnalizacji pożarowej,
– system kontroli obwodowej,
– zabezpieczenia mechaniczne i budowlane,
– system ewakuacyjny i antypanikowy.

Przy projektowaniu systemu bezpieczeństwa dla szkoły zazwyczaj główną uwagę skupia się na systemie nadzoru wizyjnego. Zwłaszcza w ostatnich latach, w wyniku powstania rządowego projektu dofinansowania montażu tego rodzaju systemów, zauważa się wzrost zainteresowania wizyjnym nadzorem szkół. Jednak same kamery nie zapewnią pełnej ochrony. System musi być kompleksowy i zapewnić ochronę przed większością potencjalnych zagrożeń. System alarmowy musi skutecznie chronić przed włamaniem, kradzieżą lub dewastacją mienia. Większość szkół posiada pracownie komputerowe wyposażone w sprzęt elektroniczny o dużej wartości, które stanowią przynętę dla potencjalnego włamywacza. System sygnalizacji pożarowej jest konieczny ze względu na dużą liczbę łatwopalnych przedmiotów znajdujących się w salach i na ścianach. Podstawowym rodzajem zabezpieczeń są zabezpieczenia mechaniczne i budowlane, które chronią przede wszystkim przed wtargnięciem na teren budynku. Zabezpieczenia mechaniczne i budowlane to kraty w oknach, drzwi i okna odporne na włamanie, zamki z atestem czy też odpowiednia organizacja pomieszczeń utrudniająca włamanie. Należy też zwrócić uwagę na oszczędności związane z posiadaniem systemu alarmowego i systemu nadzoru wizyjnego. Nadzór wizyjny dyscyplinuje uczniów, sprawia, że czują się obserwowani i nie czują się bezkarni. Tam, gdzie go zastosowano, nauczyciele stwierdzili znaczny wzrost dyscypliny uczniów oraz zmniejszenie się liczby aktów wandalizmu. W szkole z nadzorem wizyjnym uczeń nie zdecyduje się na zniszczenie sprzętu lub pomalowanie ściany. Z kolei zainstalowany system alarmowy upoważni do zniżek u ubezpieczycieli. Przykładowe zniżki w towarzystwie ubezpieczeniowym Warta w przypadku monitorowanego systemu alarmowego z załogami interwencyjnymi wynoszą 30%, zaś dzięki samym drzwiom antywłamaniowym z certyfikatem można uzyskać zniżkę rzędu 20% składki ubezpieczenia [3]. Posiadanie systemu zabezpieczeń jest po prostu opłacalne. Nowoczesna szkoła musi dbać o bezpieczeństwo swoich uczniów, a także o ich i swoje mienie.

uszczerbek na zdrowiu	udział w bójce lub pobiciu	zgwałcenie	kradzież cudzej rzeczy	kradzież z włamaniem	przestępstwa rozbójnicze	przestępstwa narkotykowe
2 208	1 021	26	2 639	650	3 918	433

Tab. 1. Liczba przestępstw popełnionych na terenie szkół podstawowych i gimnazjów w 2009 r.

uszczerbek na zdrowiu	udział w bójce lub pobiciu	zgwałcenie	kradzież cudzej rzeczy	kradzież z włamaniem	przestępstwa rozbójnicze	przestępstwa narkotykowe
139	60	7	874	159	150	291

Tab. 2. Liczba przestępstw popełnionych na terenie szkół średnich i zawodowych w 2009 r.

Rys. 1. System bezpieczeństwa obiektu dydaktycznego [2]

Analiza systemu bezpieczeństwa obiektu ma na celu sprawdzenie aktualnych zagrożeń obiektu (rodzajów zagrożeń i ich poziomu), sposobu zabezpieczenia obiektu przed występującymi zagrożeniami oraz określenie słabych i mocnych stron tych zabezpieczeń. Jest ona niezbędna przy projektowaniu nowego systemu zabezpieczeń lub modernizacji systemu istniejącego. Analiza zagrożeń obiektu może być przeprowadzona z użyciem metody ZTN-3, opracowanej i opisanej przez Z. T. Nowickiego [4]. Metoda ta ma na celu ustalenie koniecznych środków ochrony osób i mienia w przypadku występowania potencjalnych zagrożeń. Idealnie nadaje się do analizy niewielkich obiektów, takich jak szkoły czy obiekty prywatne.

Proces badawczy z wykorzystaniem metody ZTN-3 ma następujący przebieg:

1) Ustalenie:
   – zagrożeń, które potencjalnie mogą dotyczyć obiektu,
   – prawnie chronionych dóbr, które mogą być narażone,
   – miejsc prawdopodobnego wystąpienia zagrożeń.
2) Określenie słabych punktów, czyli konkretnych miejsc, które sprzyjają powstawaniu zagrożeń w obiekcie.
3) Zakwalifikowanie obiektu do kategorii zagrożonej wartości zgodnie z obowiązującą normą.
4) Wskazanie nowych środków ochrony, w tym urządzeń tworzących system alarmowy.
5) Zweryfikowanie skuteczności nowego systemu ochrony.

Podczas analizy i oceny zagrożeń przestępczych należy zwrócić szczególną uwagę na to, jakie rodzaje zagrożeń mogą dotyczyć badanego obiektu i które fragmenty obiektu są najbardziej narażone na określone zagrożenia. Szkoła może być zagrożona m.in. bójkami, pobiciami, dewastacją mienia, włamaniami, kradzieżami, wyłudzeniami, rozprowadzaniem narkotyków. Należy zlokalizować miejsca o największym prawdopodobieństwie ich zaistnienia.

Następnie należy przeanalizować stan obiektu, jego otoczenie, istniejące już zabezpieczenia oraz ich skuteczność w celu wyeliminowania słabych punktów. Należy zwrócić uwagę na umiejscowienie obiektu, historię zdarzeń przestępczych, stan jego otoczenia, ogrodzenia, oświetlenia, bram i wejść, architekturę budynku, rozmieszczenie okien, drzwi, włazów, sąsiedztwo innych budynków. Należy uporządkować otoczenie budynku, aby wyeliminować czynniki mogące sprzyjać powstawaniu zagrożeń. Ogrodzenie budynku powinno być szczelne, jego konstrukcja i ukształtowanie powinny utrudniać przedostanie się na teren obiektu bez użycia drabiny, podpórki itp. Wejścia na teren powinny być należycie oświetlone i odsłonięte, ewentualny intruz nie powinien mieć możliwości skrytego wejścia na teren szkoły. Poza tym oświetlenie powinno być takiej mocy, aby można było rozpoznać osoby na nagraniu zarejestrowanym w nocy przez kamery zewnętrzne. Jeżeli dookoła ogrodzenia znajduje się żywopłot, to powinien on sięgać co najwyżej parapetów okien na parterze [5].

Poszczególne rodzaje zagrożeń	Ocena audytu	Ocena maks.	Uwagi
Ocena zagrożenia ze względu na położenie obiektu	2	5	Budynek położony w bezpiecznej okolicy
Wpływ otoczenia na zagrożenie obiektu	2	5	Najbardziej prawdopodobny kierunek obrany przez intruza
Wpływ ogrodzenia obiektu na poziom bezpieczeństwa obiektu	3	5	Brak: 5, niewłaściwe: 3, właściwe: 1, dobre: 0
Wpływ oświetlenia budynku i obiektu na poziom bezpieczeństwa	1	5	Skuteczność oświetlenia i możliwość rozpoznania intruza – brak: 5, niewłaściwe: 3, właściwe: 1, dobre: 0
Ocena stanu wejść i bram wjazdowych na teren obiektu ze względu na możliwość zaistnienia zagrożeń	1	5	Ocena utrudnienia wtargnięcia niepożądanym osobom – brak: 5, niewłaściwe: 3, właściwe: 1, dobre: 0
Wpływ rozwiązań architektoniczno-konstrukcyjnych na możliwość zaistnienia zagrożeń przestępczych	2	5	Ocena możliwości niepostrzeżonego wtargnięcia przez drabinki, okna, balkony, włazy itp. – brak: 5, niewłaściwe: 3, właściwe: 1, dobre: 0
Ocena stanu drzwi i okien ze względu na możliwość wtargnięcia	2	5	Słabe: 5, niewłaściwe: 3, właściwe: 1, dobre: 0
Ocena zagrożeń mogących wystąpić w obiekcie			**Uwagi**
Kradzież z włamaniem	3	5	Średnie ryzyko włamania z zewnątrz oraz kradzieży
Zagarnięcie i zniszczenie mienia	3	5	Kradzieże plecaków, rowerów, wyposażenia pracowni; działania wandali
Fałszywe alarmy telefoniczne	2	5	Miało już miejsce takie zdarzenie
Wtargnięcie osób niepożądanych na teren obiektów	3	5	Duże zagrożenie ze strony handlarzy narkotyków, złodziei itp.
Dewastacja mienia	2	5	Istnieje grupa bardzo agresywnych uczniów
Zagrożenia naturalne i środowiskowe w tym zagrożenie wyładowaniami atmosferycznymi	1	5	Mało prawdopodobne, istnieje system ochrony odgromowej
Dystrybucja narkotyków	2	5	Budynek znajduje się w małej miejscowości, ale istnieje w nim problem narkotyków
RAZEM (SUMA)	**29**	**70**	
Uzyskany procent zgodności z wymaganiami	**41%**		

Tab. 3. Analiza zagrożeń obiektu

Po ustaleniu wszystkich potencjalnych zagrożeń należy określić poziom zagrożenia obiektu. Można posłużyć się skalą punktową – każdemu rodzajowi zagrożeń przyznać określoną liczbę punktów określającą ryzyko zaistnienia zdarzenia. W ten sposób można bardzo łatwo określić procentowy poziom ryzyka i kategorię zagrożenia. Przykładową analizę ryzyka prezentuje tabela nr 3. Każdemu rodzajowi zagrożeń została przypisana ocena z przedziału 0–5, co pozwala ustalić poziom zagrożenia i sklasyfikować poziom zabezpieczenia. Skala ocen jest rosnąca, czyli im wyższa ocena, tym większe ryzyko zaistnienia danego zagrożenia [6].

Po przeprowadzeniu analizy możemy ustalić procentowy wskaźnik zagrożenia obiektu. Pomaga on w ustaleniu określonej klasy zabezpieczenia obiektu, zależnej od przewidywanej wiedzy przestępców.

Klasa 1 (ryzyko małe) – oczekuje się, że włamywacze będą słabo znać systemy sygnalizacji włamania i będą zmuszeni do korzystania z ograniczonej liczby łatwo dostępnych narzędzi.

Klasa 2 (ryzyko małe do średniego) – oczekuje się, że włamywacze będą słabo znać systemy sygnalizacji włamania oraz będą używać podstawowych narzędzi i przyrządów ręcznych.

Klasa 3 (ryzyko średnie do wysokiego) – oczekuje się, że włamywacze będą biegle znać systemy sygnalizacji włamania i będą dysponować szerokim zakresem narzędzi oraz ręcznych urządzeń elektronicznych.

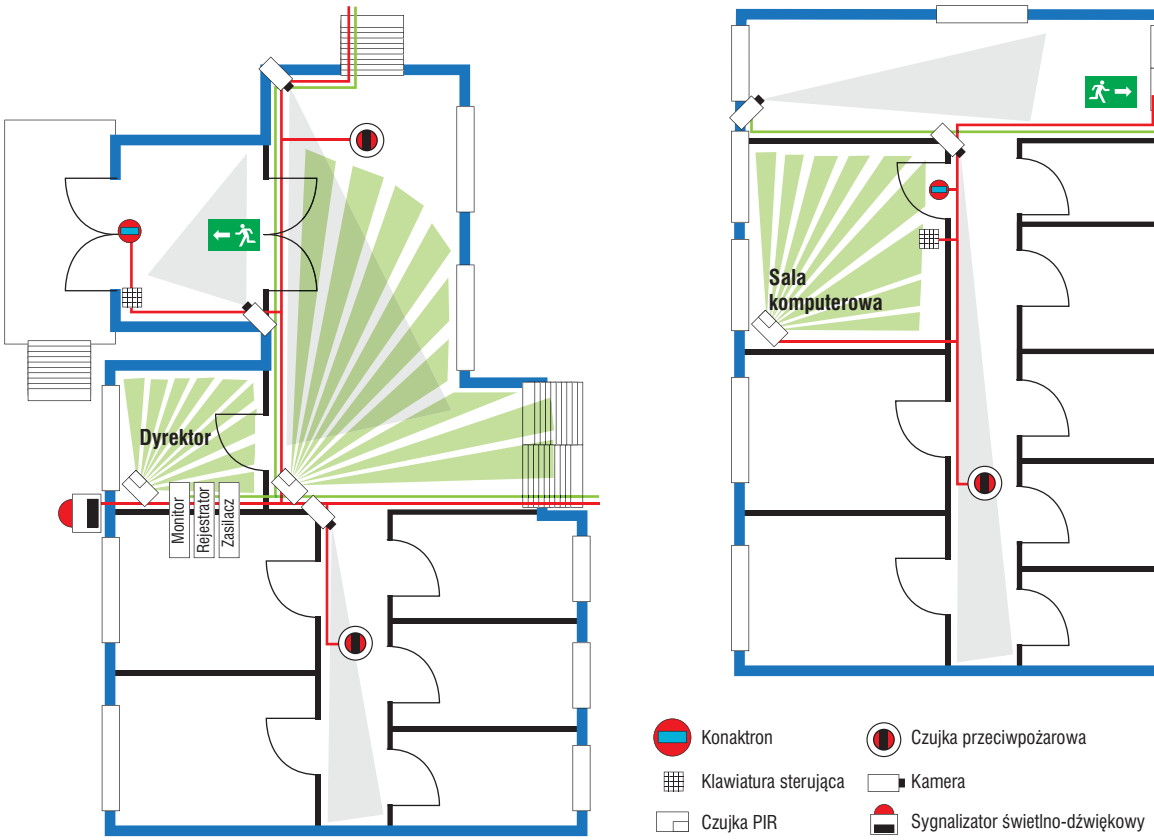
Klasa 4 (ryzyko wysokie) – oczekuje się, że włamywacze będą mieć możliwość szczegółowego zaplanowania włamania i będą dysponować pełnym zakresem urządzeń, łącznie z elementami umożliwiającymi podmianę kluczowych części składowych systemu sygnalizacji włamania.

Ze względu na specyfikę mienia, które znajduje się na terenie szkół, tego rodzaju obiektom zazwyczaj przypisuje się klasę zabezpieczenia 1 lub 2. Zazwyczaj włamania do szkół są działaniami spontanicznymi lub słabo zaplanowanymi, często dokonywanymi przez uczniów lub osoby z nimi powiązane. Dlatego też nie przewiduje się, że potencjalny włamywacz zastosuje wyrafinowane środki umożliwiające pokonanie zabezpieczeń bardziej zaawansowanych niż zabezpieczenia klasy 2. Stosowanie zabezpieczeń klasy 3 albo 4 nie ma uzasadnienia ekonomicznego.

Przy projektowaniu środków ochrony powinno się kłaść nacisk na:

– neutralizację zagrożeń w miejscach ich najbardziej prawdopodobnego wystąpienia;
– ograniczanie czynników mogących sprzyjać powstawaniu zagrożeń;
– specyfikację urządzeń, adekwatną do wymagań klasy systemu.

Filarami systemu bezpieczeństwa są system nadzoru wizyjnego oraz system sygnalizacji włamania i napadu. System nadzoru wizyjnego powinien być wyposażony w zestaw kamer podłączonych do rejestratora cyfrowego. Kamery należy umieścić w najważniejszych miejscach szkoły – tam, gdzie gromadzi się najwięcej osób, w szatniach, przy wejściach itp. System alarmowy (sygnalizacji włamania i napadu) to czujki ruchu na korytarzach i w salach komputerowych, czujki kontaktronowe w drzwiach. Aby zwiększyć bezpieczeństwo obiektu, do centrali systemu sygnalizacji włamania i napadu można podłączyć



Rys. 2. Plan przykładowego systemu alarmowego i monitoringu [7]

czujki sygnalizacji pożarowej[1]. Wiele firm ma w swojej ofercie czujki dymu, które można podłączyć do centrali alarmowej (np. Jablotron SD-280 lub OSD23). Przykładowy projekt modelowego systemu prezentuje rysunek nr 2.

Przy planowaniu rozmieszczenia urządzeń w szkołach należy pamiętać o kilku wytycznych dotyczących montażu urządzeń:

– kamery powinny obejmować możliwie największy obszar, aby wyeliminować tzw. martwe strefy (w tym celu należy stosować szerokokątne obiektywy);
– w polu widzenia kamer powinny znajdować się wszystkie „szlaki komunikacyjne" w szkole, czyli na przykład droga od wejścia do szatni, korytarze, wyjścia z terenu szkoły, klatki schodowe;
– kamery powinny być tak usytuowane, aby możliwa była pełna identyfikacja osób wchodzących do/wychodzących ze szkoły;
– pole widzenia kamer powinno być zaplanowane tak, aby kamery mogły się wzajemnie nadzorować, a osoba, która chce dostać się w dowolne miejsce w budynku, była w polu widzenia chociaż jednej kamery; osoba poruszająca się po obiekcie musi mieć świadomość takiego nadzoru,
– czujki ruchu powinny być umieszczone w taki sposób, aby potencjalny włamywacz musiał przejść przez co najmniej jedną strefę zasięgu czujki na drodze do pomieszczeń z najcenniejszymi rzeczami.

1) Oczywiście włączenie takich czujek nie spełnia wymagań przepisów o ochronie przeciwpożarowej, ale wspomaga istniejący system alarmowy, umożliwiając detekcję pożaru w wybranych miejscach – przyp. red.

Systemy bezpieczeństwa powoli stają się obowiązkowym elementem wyposażenia każdej szkoły. Troska o bezpieczeństwo uczniów, nauczycieli oraz mienia powoduje ciągły wzrost zainteresowania tymi systemami. Dyrektorzy szkół muszą wiedzieć, jak działają systemy bezpieczeństwa, aby móc je poprawnie wykorzystywać. Muszą mieć świadomość tego, że są odpowiedzialni nie tylko za bezpieczeństwo, ale także za życie i zdrowie uczniów. Dlatego warto propagować wiedzę o systemach bezpieczeństwa w szkołach. To inwestycja, która na pewno się opłaci – na bezpieczeństwie dzieci nie wolno oszczędzać.

mgr inż. Adam Rudzki

Literatura

1) *Przestępczość w szkole i innych placówkach oświatowych* (*http://www.policja.pl/portal.php?serwis=pol&dzial=4&id=4259&poz=1*)
2) Praca własna.
3) *http://www.warta.pl/dynamic/common/Artykul.jsp?aid=12348&active=1342*
4) Nowicki Z. T., *Badanie bezpieczeństwa obiektu. Zagadnienia organizacyjno-prawne*, wyd. 2 popr. i uzup., Centrum Kształcenia i Doskonalenia Kadr, Warszawa 2004.
5) Malinowski T., Piwowar R., *Monitoring w szkołach*, materiały instruktażowe Komendy Wojewódzkiej Policji w Krakowie, Kraków 2005.
6) Wójcik A., *Mechaniczne i elektroniczne systemy zabezpieczeń*, Verlag Dashöfer 2000.
7) Praca własna.

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.

RCP Master *PR602LCD*

roger®

www.roger.pl

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Wprowadzono do oferty PR411DR - nowy kontroler dostępu jednego przejścia przystosowany do montażu na standardowej szynie DIN 35mm.

Integracja systemów ochrony z procesami biznesowymi

Krzysztof Bełdycki

Potrzeba poczucia bezpieczeństwa sprawiła, że od zamierzchłych czasów człowiek woli przebywać w zorganizowanej grupie niż przemierzać świat w samotności. Przynależność do takiej grupy wiąże się z odpowiednimi zadaniami, jakie każdy z jej członków musi wykonywać, i z dostosowaniem się do panujących w niej reguł. Postępujący rozwój cywilizacyjny sprawił, że każda z grup społecznych ma wyznaczone cele, których zrealizowanie jest możliwe dzięki współpracy poszczególnych jej członków. Proces ten przyczynił się do większego zintegrowania wielu grup, doprowadzając do powstania różnych narodów. To właśnie dzięki takim procesom termin „integracja" stał się bardzo popularny i jest często używany w dziedzinie kultury, gospodarki, polityki czy informatyki. Ten ostatni przykład pokazuje, jak istotne znaczenie ma integracja w dzisiejszych czasach. Umożliwia nam ona dostęp do różnego rodzaju informacji, przydatnych w życiu prywatnym i zawodowym, oszczędzając przy tym czas i pieniądze, a także chroniąc nasze zasoby przed różnymi zagrożeniami

W zależności od tego, z jakiego rodzaju zagrożeniem mamy do czynienia, dobieramy odpowiedni zakres systemów zabezpieczeń tak, aby zminimalizować występujące ryzyko przy optymalnych nakładach, jakie możemy przeznaczyć na ten cel. Stale, od przeszło dwudziestu lat rozwijający się krajowy rynek usług ochrony umożliwia korzystanie z takich rozwiązań, jak np. stała ochrona fizyczna, ochrona doraźna, monitoring, zabezpieczenia techniczne, a także serwis recepcyjny, umożliwiając tym samym dostosowanie form ochrony adekwatnie do zagrożeń. To właśnie odpowiednio przygotowana analiza zagrożeń, jaką jest np. audyt bezpieczeństwa, umożliwia właściwy dobór systemu ochrony do danego obiektu, oparty na trzech filarach stanowiących w pełni zintegrowany system składający się z ochrony fizycznej, zabezpieczeń technicznych i procedur bezpieczeństwa. Te trzy elementy muszą być ze sobą wzajemnie powiązane i stale się uzupełniać, aby system ochrony był kompletny i skutecznie przeciwdziałał

zagrożeniom. Aby dany obiekt był szczelnie chroniony, nie wystarczy dobrze dobrany i przeszkolony personel ochrony fizycznej mający do dyspozycji bardzo zaawansowane systemy zabezpieczeń technicznych. Jeśli zabraknie odpowiednich procedur bezpieczeństwa, w systemie pojawi się luka, w wyniku której ryzyko związane z narażeniem obiektu na różnego rodzaju zagrożenia nie zostanie odpowiednio zminimalizowane. Właściwe procedury stanowią uzupełnienie dwóch pozostałych filarów bezpieczeństwa i pełnią rolę drogowskazów, jednakże wymagają ciągłej aktualizacji. Jest to naturalny proces, który powinien być okresowo powtarzany, aby można było dostosować system ochrony do aktualnych warunków, w jakich funkcjonuje dany obiekt, z uwzględnieniem takich czynników, jak rozwój biznesu klienta, postęp technologiczny, a także rodzaje zagrożeń wewnętrznych i zewnętrznych. Raz zaproponowany system ochrony nie będzie stale aktualny, podobnie jak raz przyjęta strategia rozwoju przedsiębiorstwa wymaga zmian, aby sprawnie funkcjonować i przynosić oczekiwane korzyści.

Często stosowaną i bardzo popularną formą ochrony obiektów jest usługa polegająca na ciągłym przebywaniu pracownika ochrony fizycznej na terenie chronionego obiektu. Początkowo obiekty były zabezpieczane przez liczne posterunki ochrony. Posterunki te stopniowo zastępowano systemami zabezpieczeń technicznych, takimi jak systemy kontroli dostępu czy telewizji dozorowej, co umożliwiło redukcję ich liczby i tym samym zmniejszenie narażenia pracowników ochrony na ewentualne niebezpieczeństwo. W takim systemie kluczową rolę odgrywał tzw. posterunek TV-ROOM, na którym operatorzy obsługiwali poszczególne systemy zabezpieczeń technicznych i realizowali przygotowane procedury ochrony obiektu.

Rozwój połączeń sieciowych i Internetu nie pozostał bez wpływu na technikę i organizację systemów bezpieczeństwa. Możliwości tkwiące w infrastrukturze internetowej zaczęto wykorzystywać w organizacji systemów zabezpieczeń technicznych, zapewniając globalne zarządzanie oraz optymalizację zasobów niezbędnych do ich właściwej obsługi, natomiast połączenia światłowodowe zapewniają dużą przepustowość łączy i szybkość transmisji sygnału na znaczne odległości. Poszczególne urządzenia pracujące w sieci mają przypisany adres IP, umożliwiając tym samym wzajemną komunikację. Adres IP urządzenia umożliwia jednocześnie komunikację z siecią znajdującą się poza chronionym obiektem, dzięki czemu można zrealizować zdalny nadzór urządzeń.

Rys. 1. Schemat integracji systemu ochrony z obszarami biznesu klienta – opracowanie własne

Architektura współcześnie stosowanych urządzeń umożliwia ich praktycznie bezobsługową pracę, ale analizą zarejestrowanych zdarzeń zajmują się operatorzy o wysokich kwalifikacjach. Tak naprawdę to oni zarządzają systemem, definiują bowiem zjawiska uznane za niebezpieczne, a także opracowują algorytmy reakcji systemu ochrony obiektu na takie zdarzenia.

Wdrażając opisane wyżej rozwiązanie (z wykorzystaniem infrastruktury internetowej) w obiektach sieciowych (np. w sektorze logistycznym) można uzyskać lepszy nadzór nad systemami, skrócić do minimum czas reakcji na zdarzenia oraz poprawić efektywność całego systemu ochrony. W tym przypadku integracja systemu ochrony powinna obejmować skoordynowanie procesów biznesowych z procesami bezpieczeństwa, czyli m.in. ruch osobowy, ruch samochodowy, dostawę towarów, segregowanie, czas obsługi procesu produkcyjnego. Do koordynacji procesów służy odpowiedni harmonogram, na podstawie którego można zaplanować pewne powtarzalne czynności dla danego obiektu, np. otwarcie stref dostępu, obserwację załadunku towaru czy też zarządzanie ruchem samochodowym z wykorzystaniem tablic informacyjnych, na których wyświetla się komunikat zawierający numer rejestracyjny samochodu oraz numer doku, pod który kierowca może podjechać w celu dokonania załadunku lub rozładunku towaru. Dzięki łączności radiowej lub telefonicznej operator może być w stałym kontakcie z pracownikami obiektu, jednocześnie analizując w czasie rzeczywistym raporty związane z obsługą danego procesu. Zarejestrowany przez kamery obraz wyświetlają wielkoformatowe monitory, na których operator może ustawiać interesujący go w danej chwili obraz. Przy dużej liczbie kamer niezbędne stają się funkcje inteligentnej analizy obrazu, dzięki którym system poinformuje operatora o wykrytym zagrożeniu, np. wtargnięciu do strefy chronionej czy nieautoryzowanym otwarciu doku załadunkowego. Operator może przesłać taką informację do lokalnych służb ochrony lub pracowników ochrony doraźnej w celu dokonania sprawdzenia, a jednocześnie może koordynować przebieg interwencji.

Powyższy przykład pokazuje, jak można optymalnie wykorzystać poszczególne zasoby składające się na system ochrony i skutecznie realizować powierzone zadania z tego zakresu. Nowoczesne podejście do świadczenia usług ochrony powinno w jak największym stopniu zapewnić klientowi poczucie bezpieczeństwa, ograniczać koszty prowadzenia jego działalności biznesowej poprzez redukcję strat, dostarczać w czasie rzeczywistym analizy realizowanych procesów, a przede wszystkim polegać na wspólnym osiąganiu wyznaczonych celów. Aby powiązać to wszystko ze sobą, należy już na etapie planowania danego przedsięwzięcia uwzględnić szereg istotnych elementów, które pozwolą na zaprojektowanie takiego systemu ochrony, który zintegruje procesy biznesowe z procesami bezpieczeństwa.

Krzysztof Bełdycki
Securitas Polska

Nocuj bezpiecznie

Sławomir Wagner

Branżą, która w Polsce rozwija się bardzo dynamicznie, jest hotelarstwo. Już w zamierzchłych czasach ludzie przemieszczali się, poszukując nowych miejsc, prowadząc różne interesy, handlując lub zdobywając nowe terytoria. Musieli zatem gdzieś odpoczywać. Na szlakach ich podróży powstawały obiekty, w których mogli znaleźć schronienie, posiłek i w których mogli odpocząć. Obecnie powstające obiekty hotelarskie, oprócz podstawowych funkcji, jakie mają spełniać, w niczym nie przypominają tych sprzed wieków. Przykładowa definicja hotelarstwa brzmi: „Hotelarstwo jest to działalność gospodarcza, mająca na celu zaspokajanie podstawowych potrzeb bytowych osób przebywających poza miejscem stałego zamieszkania. Są to między innymi nocleg i wyżywienie, rekreacja i rozrywka, a także bezpieczeństwo”

W tym artykule pragnę skupić się na istotnej potrzebie – potrzebie bezpieczeństwa. Słownik współczesnego języka polskiego (wydawnictwo Reader's Digest) definiuje bezpieczeństwo jako „stan psychiczny lub prawny, w którym jednostka ma poczucie pewności, oparcie w drugiej osobie lub w sprawnie działającym systemie prawnym".

Co zatem składa się na bezpieczeństwo osób korzystających z obiektów hotelarskich? Jakie są obowiązki zarządzających tego rodzaju obiektami, wynikające z obowiązującego porządku prawnego, skoro bezpieczeństwo stało się jednym z wyznaczników tej działalności gospodarczej? Z całą pewnością trzeba uznać, że elementami, od których zależy bezpieczeństwo obiektów hotelarskich, są:

– substancja architektoniczno-budowlana,
– bezpieczeństwo przeciwpożarowe,
– bezpieczeństwo medyczne,
– bezpieczeństwo IT,
– właściwa organizacja systemów zabezpieczająco-ochronnych, w tym zabezpieczeń mechanicznych, m.in. systemu kluczy, zabezpieczeń elektronicznych i ochrony fizycznej,
– ochrona danych osobowych.

Ponadto pracownicy hotelu powinni być nie tylko kompetentni, ale także mili i uśmiechnięci. Wszystko to ma sprawić, by goście obiektów hotelarskich mieli poczucie pewności oraz oparcie w personelu i w sprawnie działającym systemie hotelowym.

Jak wcześniej wspomniałem, obowiązki spoczywające na zarządzających obiektami hotelarskimi wynikają z obowiązujących uwarunkowań prawnych. A są to między innymi:

– ustawa o działalności gospodarczej,
– ustawa o usługach turystycznych,
– ustawa – prawo budowlane,
– ustawa o ochronie przeciwpożarowej,
– ustawa o ochronie osób i mienia,
– ustawa o ochronie danych osobowych,
– konwencja o odpowiedzialności osób utrzymujących hotele za rzeczy wniesione przez gości hotelowych,
– kodeks hotelarza.

Takie są składniki bezpieczeństwa, z których wynikają obowiązki ciążące na tych zarządzających obiektami hotelarskimi, którym komfort odwiedzających ich gości nie kojarzy się tylko z wyposażeniem pokoju i smaczną kuchnią.

Czy obiekty hotelarskie są bezpieczne? Czy bezpieczni są przebywający w nich goście? W wykazie wybranych miejsc popełnienia przestępstwa, prezentowanym na stronie internetowej Komendy Głównej Policji, wygląda to bardzo dobrze.

Jak wynika z przedstawionej statystyki, obiekty hotelarskie nie znajdują się w gronie miejsc popełnienia przestępstwa, chyba że zostały zakwalifikowane jako zakład usługowy. I można by się z tego cieszyć, ale prawda jest bardziej brutalna. Oto kilka przykładów negatywnych zjawisk, które wystąpiły na terenie obiektów hotelarskich:

	Zabójstwo	Uszczerbek na zdrowiu	Bójka lub pobicie	Zgwałcenie	Kradzież cudzej rzeczy	Kradzież z włamaniem	Przestępstwa rozbójnicze
budynek samodzielny	157	1 001	311	308	9 362	10 604	682
budynek wielorodzinny	326	1 978	721	432	18 300	11 590	1 989
letni dom wypoczynkowy	10	21	20	9	788	3 518	16
centrum handlowe	1	52	44	0	13 679	924	233
zakład usługowy	0	15	15	1	1 079	885	35
restauracja, bar, pub	16	785	740	7	9 394	4 367	265
sklep, butik	2	97	52	5	9 793	7 996	880
pociąg, wagon	0	18	19	3	3 064	285	83

Tab. 1. Wybrane miejsca popełnienia przestępstwa (liczba przestępstw stwierdzonych w 2009 r.)

– 2005 rok – napad rabunkowy na zakopiański hotel Wersal, dokonany przez byłą pracownicę,
– 2006 rok – napad obywatela Ukrainy na dyrektora hotelu w Katowicach,
– 2008 rok – zatrzymanie w jednym z hoteli w Bydgoszczy grupy przestępczej planującej napad na konwój,
– 2008 rok – napad rabunkowy na hotel w Zawierciu (łupem stał się dzienny utarg),
– 2009 rok – pobicie gościa hotelu w Koninie ze skutkiem śmiertelnym,
– 2009 rok – zatrzymanie w Lublinie 27-latka, który dokonał rozboju na dziewczynie i jej znajomym (sprawca najpierw pił razem z nimi alkohol w jednym z lubelskich hoteli, a następnie pobił i okradł ich z pieniędzy oraz wartościowych przedmiotów),
– 2010 rok – napad na pracownicę w hotelu w Chełmie (kobieta została pobita i zgwałcona).

Te kilka przypadków świadczy o tym, że obiekty hotelarskie oraz ich goście nie są bezpieczni. Czy te obiekty mają wypracowany system bezpieczeństwa? Być może taki system nie zapobiegnie całkowicie różnego rodzaju przestępstwom, ale na pewno zminimalizuje ryzyko ich popełnienia. A oto nam wszystkim chodzi. Dopiero po wdrożeniu takiego systemu będziemy mogli cieszyć się, że statystyka policji nie zalicza tych obiektów do miejsc popełnienia przestępstwa.

Oto zagrożenia, które mogą wystąpić w obiektach hotelarskich:
– terroryzm polityczny, kryminalny, indywidualny i zbiorowy, terroryzm z wzięciem zakładników,
– podłożenie ładunku wybuchowego lub informacja o jego podłożeniu (w Polsce, w przeciwieństwie do USA, czyn ten nie jest jeszcze traktowany na równi z aktem terrorystycznym),
– napad rabunkowy,
– kradzież z włamaniem,
– haracze i wymuszenia rozbójnicze,
– wandalizm,
– bójki i awantury (wszczynane zarówno przez gości hotelu, jak też osoby z zewnątrz, np. korzystające z restauracji),
– pożar,
– inne klęski żywiołowe (np. powódź, trzęsienie ziemi, wybuch wulkanu, huragan, tornado, ekstremalne upały lub mróz),
– zagrożenie chemiczne i biologiczne,
– włamania do systemów teleinformatycznych, kradzież danych.

Hotele bywają również miejscem:
– porachunków grup przestępczych,
– rezydowania grup przestępczych,
– zakładania podsłuchów,
– hazardu,
– handlu narkotykami,
– spożywania alkoholu,
– nierządu i sutenerstwa.

Jest to tylko cześć zagrożeń, jakie mogą dotyczyć obiektów hotelarskich. Pominąłem zagrożenia wynikające z prowadzonej działalności, takie jak wszelkiego rodzaju awarie instalacji wodnej, elektrycznej i gazowej oraz zagrożenia wynikające z problemów z dostawami usług mających bezpośredni wpływ na ciągłość pracy każdego obiektu hotelarskiego.

Co zatem zrobić, aby wyeliminować lub zminimalizować ryzyko wystąpienia któregoś z wymienionych zagrożeń? Jak wcześniej wspomniałem, dla każdego obiektu hotelarskiego należy wypracować odpowiedni system bezpieczeństwa z uwzględnieniem konkretnych uwarunkowań. Wynika to z faktu, że każdy z obiektów ma swoją specyfikę, wynikającą np. z miejsca lokalizacji, połączenia z drogami i innymi szlakami komunikacyjnymi, a także z zagrożeń występujących w danym regionie. Powinniśmy zacząć od opracowania koncepcji ochrony, która powinna uwzględniać:
– ogólne dane obiektu (położenie, właściciela, użytkownika, przeznaczenie),
– opis obiektu (sposób zabudowy, ogrodzenie, wejścia/wyjścia, wjazdy/wyjazdy, parkingi, sposób zagospodarowania terenu wewnętrznego, dobowy system pracy obiektu),
– rodzaje zagrożeń i prawdopodobieństwo ich wystąpienia,
– istniejące systemy zabezpieczenia technicznego (mechaniczne, elektroniczne, przeciwpożarowe),
– istniejące systemy ochrony fizycznej (liczbę posterunków, stan ilościowy bezpośredniej ochrony fizycznej, wyposażenie, godzinowy system pracy, system kontroli pracowników ochrony, system ochrony doraźnej – załogi interwencyjne),
– ocenę aktualnego stanu bezpieczeństwa obiektu,
– proponowane zmiany lub uzupełnienia systemu bezpieczeństwa w ujęciu wariantowym.

Kolejnym krokiem powinno być opracowanie planu ochrony na podstawie wybranego wariantu, który powinien uwzględniać:
– liczbę posterunków,
– liczbę pracowników ochrony,
– godzinowy system pracy,
– wyposażenie,
– techniczne środki ochrony i sposoby ich wykorzystania,
– zasady korzystania z ochrony doraźnej.

Nieodzownym elementem planu ochrony są instrukcje stanowiskowe. Każdy z posterunków powinien mieć opisane w instrukcji zadania wynikające z miejsca jego lokalizacji.

Kolejnym krokiem jest opracowanie procedur umożliwiających właściwą reakcję i sposób postępowania na wypadek wystąpienia zagrożeń wyspecyfikowanych w koncepcji. Dzięki procedurom każdy z pracowników obiektu hotelarskiego, w tym ochrona, ma przydzielone zadania i umie postępować w obliczu zagrożenia.

Ostatnim elementem systemu bezpieczeństwa jest przeszkolenie pracowników obiektu hotelarskiego, któremu ma służyć:
– pierwsze szkolenie po wprowadzeniu systemu bezpieczeństwa,
– cykliczne szkolenia ze znajomości i przestrzegania procedur (np. raz w roku),
– szkolenia nowych pracowników.

Dobry system bezpieczeństwa jest mocny dlatego, że każdy z jego elementów jest właściwie zdefiniowany, ma wypra-

cowane mechanizmy przeciwdziałania, jest systematycznie udoskonalany i realizowany przez kompetentny personel.

Zarządzający obiektami hotelarskimi powinni wypracować systemy bezpieczeństwa odpowiednie dla ich obiektów. Ważne jest to, jaki jest poziom danego systemu i przez kogo został on opracowany. Z moich spotkań z hotelarzami wynika, że problemowi bezpieczeństwa poświęca się zbyt mało uwagi. Bardzo często mówi się o kosztach, zwłaszcza w związku z kryzysem, który powoduje, że koszty związane z zapewnieniem ochrony są na pierwszym miejscu listy kosztów obciążających działalność każdej firmy. Hotelarze bardzo rzadko korzystają z usług niezależnych ekspertów, rzeczoznawców z zakresu bezpieczeństwa, w celu określenia optymalnych warunków bezpieczeństwa swoich obiektów, zaś audyty bezpieczeństwa należą do rzadkości.

Z wieloma z wymienionych zagrożeń nie mieliśmy do czynienia w Polsce, co nie znaczy, że ten pierwszy raz kiedyś nie nastąpi. Żyjemy w świecie, w którym intensywny przepływ ludzi i negatywnych zjawisk zmusza nas do dbania o swoje bezpieczeństwo, nie tylko zewnętrzne, ale także wewnętrzne.

Co powinno zmobilizować hotelarzy w najbliższym czasie? Na pewno zbliżające się mistrzostwa Europy w piłce nożnej EURO 2012. Jakie są wyzwania dla zarządzających obiektami hotelarskimi i z czego one wynikają? Są to:

– duża liczba osób, na którą składają się ekipy drużyn uczestników mistrzostw, kibice, zaproszeni oficjele i goście, ekipy obsługi medialnej (prasa, radio, telewizja), ekipy obsługi technicznej oraz pracownicy służb porządkowych i informacyjnych,
– wielonarodowość i wynikające z niej różnice językowe, kulturowe i wyznaniowe,
– krótkotrwałość pobytu wynikająca z kalendarza rozgrywek.

Baza hotelowa w Polsce, pomimo jej dynamicznego rozwoju, pozostawia wiele do życzenia. Trzeba mieć nadzieję, że do momentu otwarcia mistrzostw nastąpi jej powiększenie i ulepszenie. Już teraz podpisywane są kontrakty z hotelami dotyczące pobytu ekip drużyn uczestników, oficjeli i gości. Te obiekty muszą zatem spełnić najwyższe standardy bezpieczeństwa wyznaczone przez organizatora turnieju – UEFA.

Trudno też wyobrazić sobie pobyt kibiców dwóch zwaśnionych drużyn w jednym hotelu (np. kibiców angielskich i niemieckich), biorąc pod uwagę mecz 1/8 finału mistrzostw w RPA i nie uznaną przez sędziego, prawidłowo strzeloną bramkę.

Bariera językowa, kulturowa i wyznaniowa to dodatkowe wyzwanie. Krótkotrwały pobyt kibiców poszczególnych ekip wiąże się z dodatkowym wysiłkiem w celu zapewnienia nie tylko komfortu, ale także bezpieczeństwa obiektowi, gościom i ich mieniu.

Każdy z nas chce, aby pobyt w hotelu dawał mu poczucie pewności, że jemu, jego bliskim i jego mieniu nic złego się nie stanie, że swój samochód zastanie w tym samym miejscu, w którym go pozostawił. Ktoś musi czuwać, byśmy mogli spokojnie spać. Wcale nie musi to być policja. Wystarczy, że zarządzający obiektami hotelarskimi wypełnią swój obowiązek – zapewnią bezpieczeństwo gościom i ich mieniu.

Sławomir Wagner
WAGPOL

Rejestracja obrazu z kamer HD

Tomasz Polus

Nowe technologie mamy zwyczaj określać wieloma nazwami roboczymi do czasu, kiedy jedną z nich przyjmiemy za standard. Tak samo jest w przypadku nowoczesnych kamer do telewizji przemysłowej, które nazywamy obecnie kamerami megapikselowymi i kamerami HD. Oba te określenia odnoszą się do kamer sieciowych (kamer IP), które oferują rozdzielczość obrazu 1,3 Mpix lub wyższą. Dlatego nazwy te można stosować zamiennie – zarówno w stosunku do urządzeń telewizji komercyjnej, jak i przemysłowej. Gdybyśmy przyjęli tylko jedno z tych określeń, byłoby prościej

Rozdzielczość kamer HD odpowiada bezpośrednio rozdzielczości kamer przemysłowych. Zależnie od formatu obrazu, rozdzielczość 1,3 Mpix w kamerze megapikselowej może oznaczać 1280×960 lub 1280×1024. Są to rozdzielczości zbliżone do 1280×720, którą zwykle przyjmuje się za standard HD Ready 720p. Natomiast rozdzielczość Full HD 1080p (1920×1080) jest zbliżona do 2 Mpix. Dlaczego więc nie ujednolicić nazewnictwa?

Zwiększenie rozdzielczości obrazu do poziomu HD, oprócz oczywistych korzyści, powoduje także pewne problemy związane z przetwarzaniem dużo większej ilości danych. Problemy te dotyczą archiwizacji, szybkości zapisu i transmisji obrazów. Przekłada się to m.in. na konieczność zakupu kosztownych macierzy dyskowych i budowania szybkich sieci, co w oczywisty sposób decyduje o zwycięstwie lub porażce w przetargu.

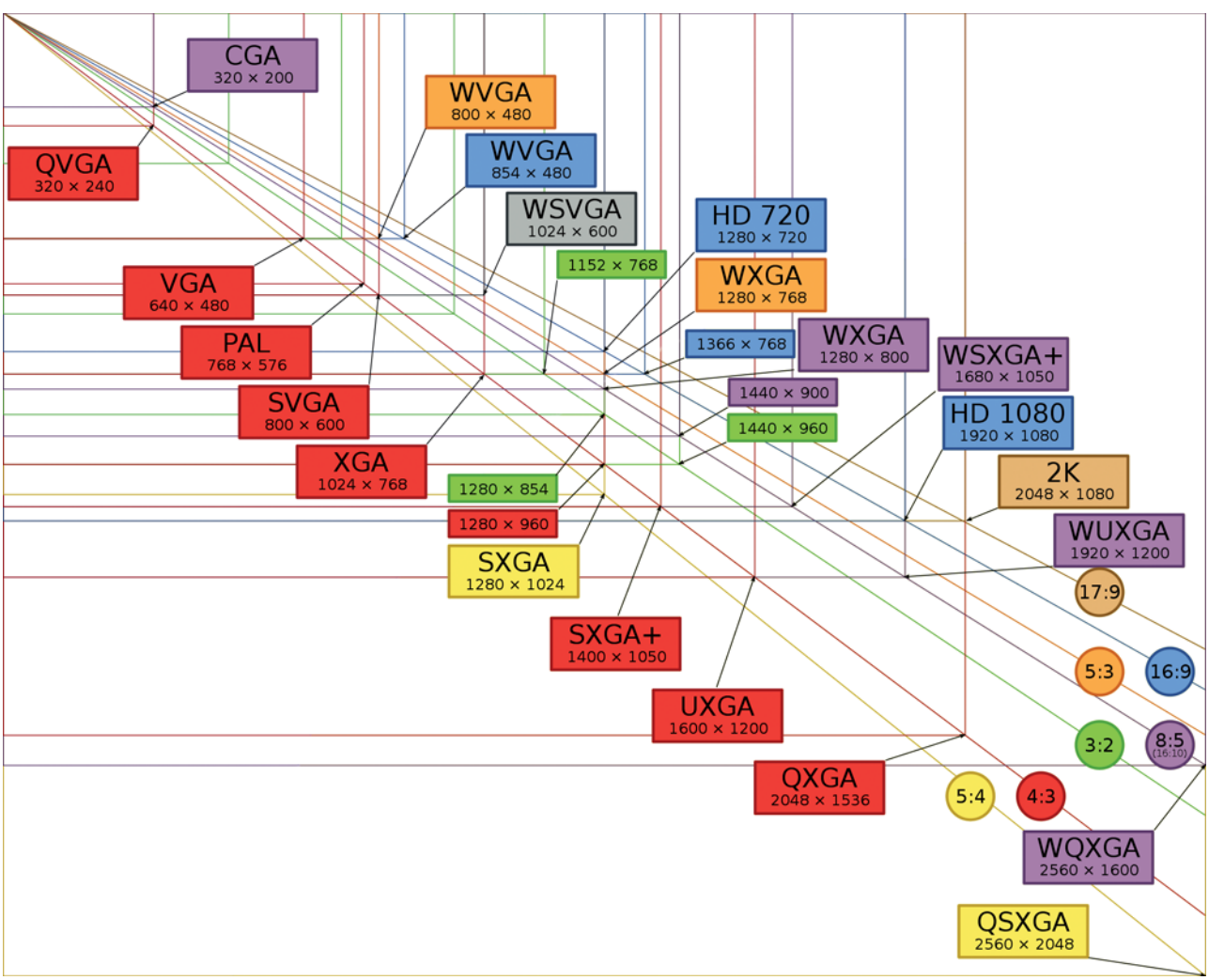
Na szczęście nowoczesna kompresja H.264 pozwoliła uciec od tych problemów dzięki kilkukrotnemu zredukowaniu ilości danych w stosunku do kompresji MJPEG przy zachowaniu porównywalnej jakości obrazu. Z praktyki wynika, że różnica w rozmiarze strumienia danych typowo wynosi od kilkunastu Mbit/s do kilku Mbit/s.

W oparciu o własne doświadczenia, w tabeli nr 1 zgromadziłem szacunkowe rozmiary strumieni wideo z typowych kamer HD. Aby uzyskać te same wartości w megabajtach na sekundę (MB/s), wystarczy podzielić poniższe wartości przez 8.

Trzeba pamiętać, że unowocześnienie metod kompresji musi dotyczyć nie tylko kamer IP, ale również rejestratorów, stacji monitorowania i oprogramowania, które jest w nich zainstalowane. Niezbędny jest kompletny system monitoringu działający zgodnie z nowymi standardami.

Warto jeszcze zwrócić uwagę, że wykorzystanie wysokiej rozdzielczości kamer HD w podglądzie na żywo jest niepełne nawet przy zastosowaniu monitorów Full HD (1920×1080). Jest to spowodowane faktem, że już podstawowy podział ekranu na cztery części wydzieli dla jednej takiej kamery 25% powierzchni monitora, czyli pole o rozdzielczości 960×540. Ta powierzchnia jest znacznie mniejsza niż obraz o rozdzielczości 1,3 Mpix (1280×960 lub 1280×1024). W takich warunkach operator systemu nie wykorzysta podczas podglądu wszystkich szczegółów oferowanych nawet przez podstawową kamerę HD, nie mówiąc już o kamerach o wyższej rozdzielczości. Dopiero włączenie funkcji cyfrowego zoomu (powiększenia fragmentów obrazu) pozwoli operatorowi w pełni wykorzystać rozdzielczość HD. Rejestrator musi jednak udostępniać tego rodzaju cyfrowe funkcje, np. Picture-in-Picture (PiP) czy Picture-and-Picture (P&P).

Dlatego w oparciu o kilkuletnie doświadczenia z rejestracją obrazu z kamer HD certyfikowaliśmy dwa modele rejestratorów sieciowych dla kamer HD: RANVR (wersja podstawowa) i RPNVR (wersja profesjonalna).



Rys. 1. Zestawienie typowych rozdzielczości obrazu

Klatki/s	Metoda kompresji	1,3 MPix (1280x1024)	2,0 MPix (1600x1200)	3,0 MPix (2048x1536)	5,0 MPix (2596x1944)
10	MJPEG	ok. 10 Mbit/s	ok. 13 Mbit/s	ok. 20 Mbit/s	ok. 30 Mbit/s
	H.264	ok. 1,5 Mbit/s	ok. 2 Mbit/s	ok. 4 Mbit/s	ok. 5 Mbit/s
15	MJPEG	ok. 15 Mbit/s	ok. 19 Mbit/s	ok. 30 Mbit/s	ok. 43 Mbit/s
	H.264	ok. 2,5 Mbit/s	ok. 3 Mbit/s	ok. 5 Mbit/s	ok. 7 Mbit/s
25	MJPEG	ok. 24 Mbit/s	ok. 31 Mbit/s	ok. 49 Mbit/s	ok. 72 Mbit/s
	H.264	ok. 4 Mbit/s	ok. 5 Mbit/s	ok. 8 Mbit/s	ok. 12 Mbit/s

Tab. 1. Szacunkowe rozmiary strumieni wizyjnych z typowych stacjonarnych kamer HD

Jedną z podstawowych zalet w odniesieniu do kamer HD jest to, że rejestratory te umożliwiają wykorzystanie od dwóch do ośmiu monitorów Full HD w trybach matryc wizyjnych, sekwencji matryc wizyjnych, okien alarmowych lub spotowych oraz map synoptycznych. Ponadto rejestratory udostępniają funkcje cyfrowego zoomu. Podczas podglądu na żywo na wielu monitorach operator może zatem w pełni wykorzystać wysoką rozdzielczość kamer HD.

Rejestratory RANVR i RPNVR bazują na zaawansowanym oprogramowaniu firmy GeoVision i systemie operacyjnym Windows XP w specjalizowanej wersji Embedded (wszystko w polskiej wersji językowej). Ze względu na wymaganą wysoką bezawaryjność urządzenia oprogramowanie jest instalowane w pamięci półprzewodnikowej. Poza standardowym nagrywaniem obrazu telewizyjnego rejestratory te oferują szereg zaawansowanych funkcji, które umożliwiają zwycięstwo nawet w najbardziej skomplikowanym przetargu. Pełną listę funkcji rejestratora RPNVR można znaleźć pod adresem: *http://www.polvision.com.pl/products.asp?lang=pl&id=227*.

Aktualna lista obsługiwanych kamer IP i wideoserwerów obejmuje urządzenia takich firm, jak ACTi, Arecont Vision, Axis Communications, Bosch, Canon, Geovision, Hikvision, IQinVision, JVC, Mobotix, Panasonic, Pelco, Sanyo, Sony, Vivotek, Verint. Dodatkowo, w ciągu najbliższych paru miesięcy, rejestratory te zostaną certyfikowane jako współpracujące z urządzeniami w nowym standardzie ONVIF.

Doskonale wentylowane i filtrowane obudowy RACK 19" 4U mogą pomieścić od pięciu do ośmiu dysków (2 TB) w kieszeniach typu hot-swap. Uzyskana pojemność 16 TB pozwala na przechowanie nagrań z wielu miesięcy. Ponadto rejestratory RANVR i RPNVR współpracują z macierzami sieciowymi (np. iSCSI) – zarówno przy zapisie nagrań, jak i przy automatycznym tworzeniu kopii zapasowej nagrań, realizowanej zgodnie ze zdefiniowanym harmonogramem.

Nagrania są archiwizowane w popularnych formatach graficznych (AVI, JPG itd.), w łatwo dostępnej i schematycznej strukturze folderów. Logi zdarzeń (np. detekcji ruchu, utraty sygnału wizyjnego) są zapisywane w standardowych, łatwych

Rys. 2. Rejestrator RPNVR

do przetwarzania bazach MDB (standard aplikacji Microsoft Office – Access). Taka organizacja danych, otwarta architektura i dostępność pakietu SDK umożliwiają integrację z praktycznie dowolnymi aplikacjami/systemami (np. fiskalnymi, wagowymi, drogowymi).

Nadzwyczajną funkcją jest też możliwość zwielokrotniania strumieni IP generowanych przez rejestrator. Przydaje się to na przykład w takich aplikacjach, w których rejestrator wysyła jedną kopię strumieni przez wolne łącze do Internetu, a zainstalowane tam serwery dystrybucyjne na szybkich łączach duplikują strumienie i dostarczają je dużej grupie odbiorców.

W instalacjach bazujących na wielu rejestratorach wykorzystuje się niezwykle rozbudowany system uprawnień, który umożliwia przechowywanie kont użytkowników systemu w centralnej sieciowej bazie danych. Rejestratory automatycznie uzyskują informacje o uprawnieniach użytkowników, łącząc się przez sieć IP z bazą. Można sobie wyobrazić, jak bardzo upraszcza to operacje związane z przydzielaniem uprawnień i zmianą haseł w sieci rejestratorów. Równie istotnym ułatwieniem w pracy administratorów systemu jest zdalne sterowanie rejestratorami przez sieć IP (tzw. zdalny pulpit).

W przetargach coraz częściej pojawiają się też wymagania związane z inteligentną analizą obrazów. Nie bez znaczenia są zatem następujące funkcje dostępne w rejestratorach RANVR i RPNVR: wykrywanie intruzów, sabotażu kamer, kradzieży i pozostawienia obiektów, zliczanie obiektów i ludzi, automatyczne śledzenie ruchomych obiektów kamerami PTZ. Za dodatkową opłatą można doposażyć rejestratory w inne funkcje, m.in. łączenie widoków z wielu kamer, redukcję efektów mgły, dymu i opadów, stabilizację obrazu, wykrywanie tłumu.

Podsumowując – profesjonalne nagrywanie obrazu z wielu sieciowych kamer HD wymaga posiadania specjalistycznego rejestratora sieciowego (NVR). W przeciwieństwie do ogromnej liczby kamer HD na rynku wciąż niewiele jest rejestratorów, które potrafią w zaawansowany sposób nagrywać obrazy z wielu kamer o wysokiej rozdzielczości. Tego rodzaju urządzenia wymagają zastosowania skomplikowanego oprogramowania i bardzo wydajnych podzespołów, tym bardziej jeśli oprócz nagrywania wideo mają realizować funkcje analizy obrazu i obsługiwać sieciowe stacje monitorowania.

Tomasz Polus
kierownik projektów w firmie POLVISION
tomek@polvision.pl

Komentarz redakcyjny

Zwracamy Państwa uwagę na dane zamieszczone w tabelce. Wynika z nich niemal liniowa zależność wielkości strumienia danych, generowanego przez kamery megapikselowe, od liczby klatek obrazowych wytwarzanych w ciągu sekundy. Niewątpliwie jest to prawdziwe w przypadku kompresji pełnoklatkowej, czyli stanowiącej pochodną metody JPEG, stosowanej do kompresji nieruchomych obrazów fotograficznych, tymczasem z tabelki wynika, że dotyczy to wszystkich metod kompresji, z różnicowymi włącznie.

Śpieszymy z wyjaśnieniem, że tego typu sytuacja jest możliwa jedynie w pewnych szczególnych warunkach, na przykład podczas obserwacji całkowicie statycznych obrazów, w których kolejne klatki są jednakowe lub niemal jednakowe. Trudno odmówić użyteczności temu sposobowi myślenia, gdyż bardzo wiele kamer pracujących w systemach monitoringu przez długie godziny obserwuje niezmiennie te same sceny, jednakże w przypadku kamer z opcją PTZ, a także podczas obserwacji ruchliwych obszarów takie myślenie całkowicie zawodzi.

We współczesnych kamerach sieciowych z kompresją różnicową można się spotkać z dwoma sposobami ustalania momentów generacji klatek różnicowych. Pierwszym z nich jest wykorzystanie parametru GOP (Group of Pictures), który określa, ile klatek różnicowych przypada na jedną klatkę referencyjną. Często parametr ten przyjmuje wartość 30, co oznacza, że w przypadku dziesięciu klatek na sekundę klatka referencyjna powtórzy się co trzy sekundy. W tym czasie w obserwowanym obrazie mogą zajść daleko posunięte zmiany (kamera PTZ może w tym czasie całkowicie zmienić pole widzenia), które spowodują, że różnice pomiędzy kolejnymi klatkami będą na tyle duże, że realizacja algorytmu kompresji różnicowej okaże się niemożliwa i kamera wygeneruje dodatkowe klatki o statusie klatek referencyjnych. Oznacza to, że wypadkowy strumień danych nie będzie tak niski, jak wynikałoby z zależności liniowej.

Drugą powszechnie stosowaną metodą jest arbitralne ustalanie, że klatka różnicowa musi być wygenerowana w określonym czasie, na przykład co sekundę. W tym przypadku proporcjonalna zależność między wielkością wyjściowego strumienia danych a liczbą klatek na sekundę w ogóle nie zachodzi, niezależnie od treści obserwowanego obrazu. Przy pewnej liczbie klatek na sekundę, w praktyce mieszczącej się w zakresie od 10 do 15, występuje zauważalne minimum. Dalsze zmniejszanie poklatkowości powoduje wzrost wielkości strumienia danych, tak więc zastosowanie zależności liniowej nie znajduje uzasadnienia.

We współczesnych kamerach sieciowych na ogół jest opcja o stałej wartości strumienia danych, w ramach której procesor zarządzający pracą kamery tak dostosowuje parametry kompresji, by w pełni wykorzystać limit dostępnego pasma sieciowego, co w praktyce oznacza, że liczba klatek transmitowanych w ciągu sekundy nie ma wpływu na wielkość generowanego strumienia danych.

Andrzej Walczyk
Redakcja

18× HDTV > 36× 4CIF

W świecie nadzoru wizyjnego mniej znaczy więcej, a 18-krotny zoom optyczny w kamerze HDTV daje lepszy efekt od 36-krotnego powiększenia 4CIF

Agata Majkucińska

W sektorze systemów monitoringu wizyjnego możliwość takiego powiększenia i skalibrowania obrazu w celu precyzyjnego zidentyfikowania szczegółów jest wartością kluczową i niejednokrotnie warunkiem wykorzystania materiału wizyjnego w procesach sądowych czy dochodzeniach. Rozpoznanie twarzy czy dostrzeżenie szczegółów ubioru osób zarejestrowanych za pomocą kamery wielokrotnie przesądzało o rozstrzygnięciu śledztwa, czy wręcz o orzeczeniu winy. Wysoka rozdzielczość obrazu w połączeniu z odpowiednim obiektywem o zmiennej ogniskowej zastosowanym w kamerze cyfrowej sprawi, że żaden detal nie umknie uwadze obserwatora.

Choć zwykło się uważać, że to najwyższa wartość powiększenia obrazu gwarantuje najlepsze efekty, doświadczenie firmy Axis Communications wskazuje na to, że – paradoksalnie – w obszarze nadzoru wizyjnego 18-krotny zoom optyczny w kamerze o rozdzielczości HD co najmniej równa się, a wręcz przewyższa możliwości modeli wyposażonych w obiektywy z dwukrotnie wyższym zakresem powiększenia optycznego, pracujące w standardzie 4CIF. Sytuację tę wyjaśnia porównanie poniższych ilustracji:

Rysunek 1 przedstawia widok przybliżony 36-krotnie za pomocą kamery obrotowej (PTZ) w rozdzielczości 4CIF (704×480 pikseli). Rysunek 3 przedstawia widok przybliżony 18-krotnie za pomocą kamery obrotowej HDTV 720p PTZ w rozdzielczości 1280×720 pikseli. W obu przypadkach rozdzielczość kamery pozwala odczytać nazwę gazety czytanej przez mężczyznę, jednak kamera HDTV oferuje tę samą ilość detali, dysponując dwukrotnie mniejszym zakresem zmian ogniskowej obiektywu niż kamera w standardowej rozdzielczości.

Kamery o rozdzielczości obrazu HD mają przewagę również ze względu na szersze pole widzenia w popularnym formacie szerokoekranowym o proporcjach 16:9, pozwalające na monitorowanie większego obszaru z wysoką szczegółowością i w wysokiej rozdzielczości. Różnicę tę obrazuje porównanie rysunków 1 i 3. Na tym ostatnim można wciąż z powodzeniem rozróżnić detale, takie jak nagłówki w gazecie, choć zarejestrowany jest znacznie szerszy kadr. Większe pole widzenia w trybie przybliżenia sprawia także, że śledzenie obiektów za pomocą kamery jest znacznie prostsze, ponieważ redukuje ryzyko wypadnięcia osoby lub przedmiotu z kadru podczas obracania kamerą.

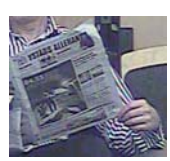
Dlaczego kamera z obiektywem pozwalającym na 18-krotną zmianę ogniskowej może wytwarzać obraz o takiej samej rozróżnialności szczegółów, jak kamera z obiektywem zapewniającym dwukrotnie większy zakres zmian ogniskowej?

Panuje powszechne przekonanie, że większy zakres zmian ogniskowej obiektywu kamery pozwala mocniej przybliżyć scenę i sprawia, że detale są bardziej widoczne. Powyższe porównanie wykazuje, że nie zawsze jest to prawda.

Obiektyw, zwany potocznie zoomem, jest układem soczewek, który ma możliwość zmiany ogniskowej. Dłuższa ogniskowa oznacza większe powiększenie, ale także proporcjonalne zmniejszenie kąta widzenia.

Zdolność obiektywu do optycznego powiększania obrazu jest zwykle wyrażana stosunkiem pomiędzy najdłuższą a najkrótszą ogniskową. Na przykład o obiektywie zapewniającym możliwość zmiany ogniskowej w zakresie od 50 mm do 200 mm mówi się, że jest to obiektyw z 4-krotnym zoomem bądź obiektyw z zoomem 4:1. Inaczej rzecz ujmując, zastosowanie najdłuższej ogniskowej dostępnej dla tego obiektywu zredukuje kąt widzenia do około jednej czwartej w stosunku do najszerszego kąta. Dwa różne obiektywy o tym samym współczynniku zmian ogniskowej mogą pracować inaczej ze względu na bezwzględną długość ogniskowej, a zatem i powiększenie. Ponadto obiektyw z większym współczynnikiem zmian ogniskowej nie musi ko-

Rys. 1. Pełen kadr z kamery w standardzie 4CIF z 36x zoomem



Rys. 2. Wykadrowany fragment zdjęcia z kamery w standardzie 4CIF z 36x zoomem

Rys. 3. Pełen kadr z kamery w standardzie HDTV z 18x zoomem

Rys. 4. Wykadrowany fragment zdjęcia z kamery w standardzie HDTV z 18x zoomem

niecznie dysponować większymi możliwościami powiększenia. Dla przykładu – obiektyw pozwalający na zmianę ogniskowej w zakresie od 15 mm do 150 mm, a więc dysponujący możliwością 10-krotnej zmiany długości ogniskowej, będzie miał w rzeczywistości słabsze przybliżenie aniżeli obiektyw z możliwością 4-krotnej zmiany ogniskowej w zakresie od 50 mm do 200 mm, bowiem ogniskowa równa 200 mm oferuje większe przybliżenie niż ogniskowa równa 150 mm.

Podobnie jak w przypadku współczynników przybliżenia, określanie powiększenia tylko za pomocą ogniskowej może być mylące. Kamera 4CIF użyta do zrobienia powyższych przykładowych zdjęć posiada dłuższą ogniskową niż kamera HDTV 720p. Dlaczego zatem rozróżnialność szczegółów na powiększonych obrazach jest podobna? Odpowiedź na to pytanie można uzyskać przez porównanie, jak kamery pracują w trybie szerokokątnym, to znaczy przy użyciu najmniejszych ogniskowych, a więc bez przybliżenia.

W obydwu przypadkach pole widzenia jest niemal identyczne, jednak łatwo zauważyć wyższą rozdzielczość i lepsze odwzorowywanie kolorów w przypadku kamery HDTV. Obrazy dostarczane przez kamerę HDTV są ostre, wyraźne i pełne szczegółów. Wystarczy porównać wycięte widoki na rysunkach 6 i 8. Liczby na tablicy wyników są widoczne na obrazie HDTV, natomiast na obrazie z kamery 4CIF są ledwo dostrzegalne.

Te zdjęcia pokazują, że w trybie szerokokątnym kamera HDTV oferuje o wiele lepszą rozróżnialność szczegółów niż kamera 4CIF. W rzeczywistości kamera HDTV dysponuje dwukrotnie większą liczbą pikseli dla tego samego pola widzenia.

W trybie pracy z maksymalną wartością ogniskowej kamery HDTV i 4CIF generują obrazy o zbliżonej rozróżnialności szczegółów, ale kamera HDTV zapewnia szersze pole widzenia.

Przeprowadzona analiza bezsprzecznie wskazuje na to, że porównywanie powiększenia obrazu wytwarzanego przez kamery tylko na podstawie współczynnika powiększenia może być mylące. Konieczne jest również uwzględnienie rozdzielczości kamery. W porównaniu do standardowej kamery 4CIF kamera HDTV o rozdzielczości 1280×720 pikseli oferuje od dwóch do trzech razy więcej pikseli w każdej klatce. To właśnie dzięki wyższej rozdzielczości kamera HDTV pracuje równie dobrze przy ograniczonym zakresie zmian ogniskowej. W rzeczywistości kamery obrotowe o wysokiej rozdzielczości mogą być stosowane na różne sposoby – można zachować takie same pole widzenia jak w kamerze o rozdzielczości 4CIF i poprawić rozróżnialność szczegółów, jak w przypadku użytej tutaj kamery HDTV, lub zwiększyć pole widzenia przy takiej samej rozróżnialności szczegółów obrazu, jak w przypadku standardowych kamer.

Jakość obrazu nie zależy wyłącznie od rozdzielczości mierzonej w pikselach. Inne cechy, takie jak ogólna jakość obiektywu czy właściwości i jakość szkła w osłonie kopuły, mają ogromny wpływ na odwzorowywanie obrazu. Równie ważne jest zagwarantowanie szybkiej transmisji strumieniowej materiału wizyjnego, dzięki której można zarejestrować i zapisać akcje mające miejsce w scenie, a także dostrzec szybko przesuwające się obiekty. Kamera HDTV, która jest zgodna z normami SMPTE pod względem rozdzielczości, poklatkowości, odwzorowania barw i proporcji obrazu, zapewnia bogate w szczegóły i wierne zdjęcia, gwarantując, że nic nie umknie uwadze.

Podsumowując – kamery HDTV spełniają bezwzględne wymagania w zakresie nadzoru wizyjnego, mając o połowę mniejszy zakres zmian ogniskowej obiektywu. Nie ulega zatem wątpliwości, że w tym przypadku mniej (pozornie) znaczy więcej.

Agata Majkucińska
Axis Communications

Rys. 5. Obraz z kamery 4CIF z 36x zoomem w trybie szerokokątnym

Rys. 6. Wycięty fragment obrazu z kamery 4CIF z 36x zoomem w trybie szerokokątnym

Rys. 7. Obraz z kamery HDTV 720p z 18x zoomem w trybie szerokokątnym

Rys. 8. Wycięty fragment obrazu z kamery HDTV 720p z 18x zoomem w trybie szerokokątnym

Inaczej rozumiana jakość obrazu to jego **użyteczność.**

Jakość obrazu jest zawsze ważna, lecz rzeczywiste korzyści jakie czerpiemy z zastosowania systemów nadzoru wideo zależne są od tego jak wykorzystujemy dane obrazy. Czy będą one ogólnie przeglądane czy też będziemy szukać detali? Czy będziemy chronić zadany obszar czy też rozpoznawać tablice rejestracyjne? Przeglądanie, nagrywanie czy też obydwie funkcje jednocześnie? Czy materiał wizyjny jest zoptymalizowany do naszych potrzeb?

Ułatwiamy pracę naszym klientom, gdyż koncentrujemy się na użyteczności materiału wizyjnego. Dzielimy się naszym doświadczeniem i kompetencjami, oferujemy szeroki zakres funkcjonalności związanych z poszerzaniem możliwości obrazu wideo takich jak zbliżanie, ogniskowanie, technologia megapikselowa i HDTV. Mogą oni w pełni korzystać z najszerszego na rynku portfolio produktów do sieciowego nadzoru wizyjnego.

W celu zapewnienia dostępu do istotnych ekspertyz dotyczących nadzoru IP w zakresie instalacji i wsparcia technicznego, dysponujemy siecią 24 000 partnerów, specjalistów Axis na całym świecie. Jako światowy lider w sieciowych systemach wizyjnych, mamy na celu pomoc w uzyskaniu maksymalnych możliwości systemów nadzoru wizyjnego naszych klientów.

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

Kamera sieciowa AXIS Q1755:
H.264, zoom i jakość obrazu HDTV.

AXIS®
COMMUNICATIONS

Niewielki i skuteczny rejestrator Aper serii PDR-XM

Mariusz Witulski

W myśl zasady „szybciej, więcej, lepiej” na rynku CCTV pojawiają się coraz wydajniejsze urządzenia rejestrujące. Większa prędkość zapisu i transmisji sieciowej oraz większa liczba wykonywanych operacji wymagają zastosowania szybszych procesorów i wydajniejszych kodeków wizyjnych. Możliwość rejestracji kilkuset klatek obrazu na sekundę przy maksymalnych rozdzielczościach jest okupiona znacznie wyższą ceną urządzeń. Niemniej w większości przypadków stosowanie drogich urządzeń w małej i średniej wielkości instalacjach nie znajduje uzasadnienia ekonomicznego. W systemach tych bardzo dobrze sprawdzają się natomiast rejestratory Aper serii PDR-XM

Rejestratory PDR-XM zostały wprowadzone na rynek pod koniec minionego roku i już znalazły szerokie uznanie wśród klientów i użytkowników. Są one optymalnym rozwiązaniem dla większości klasycznych instalacji systemów nadzoru wizyjnego, zapewnią bowiem dostateczną wydajność zapisu, a jednocześnie oferują wiele funkcji wyższych modeli rejestratorów linii PDR.

PDR-XM występuje w wersji 4-, 8- i 16-kanałowej. Urządzenia tej serii należą do klasy rejestratorów autonomicznych, działających na bazie systemu Embedded Linux. Platforma ta gwarantuje stabilność, bezpieczeństwo i niezawodność pracy. PDR-XM jest w stanie wykonywać cztery operacje jednocześnie: rejestrację, podgląd na żywo/odtwarzanie, archiwizację i transmisję sieciową (czyli jest to tzw. kwadrupleks).

Podstawowa obsługa odbywa się za pomocą monitora głównego podłączonego do wyjścia wizyjnego Video (BNC) lub do wyjścia VGA. Sterowanie rejestratorem i jego konfiguracja są realizowane poprzez proste i intuicyjne menu ekranowe w języku polskim. Proces wstępnego przygotowania urządzenia do pracy jest wydatnie skrócony przez mechanizm szybkiej konfiguracji (*Quick Setup*).

Dodatkowo, niezależnie od wymienionych funkcji, realizowanych za pośrednictwem monitora głównego, na monitorze pomocniczym (tzw. spot-monitorze) jest dostępny podgląd na żywo obrazu z pojedynczych kamer: na żądanie, w trybie alarmowym lub w sekwencji.

Kontrola nad PDR-XM może być sprawowana na wiele sposobów, zarówno lokalnie, jak i zdalnie. Do sterowania lokalnego służy dotykowa klawiatura umieszczona w panelu przednim,

Fot. 1. Ekran główny

Fot. 2. Menu ekranowe

mysz USB lub pilot IR, który jest dostarczany w komplecie z rejestratorem.

Zdalny dostęp do rejestratorów przez sieć IP można uzyskać za pośrednictwem przeglądarki internetowej (połączenie z pojedynczą jednostką), bezpłatnego oprogramowania sieciowego CMS-Lite, xCMS-DVRPlayer lub EMS (nadzór nad – odpowiednio – 1, 10 lub 1000 jednostek). Oprogramowanie pozwala na zarządzanie pracą i pełną konfigurację urządzenia, wyświetlanie i nagrywanie obrazu w czasie rzeczywistym, manewrowanie kamerami obrotowymi, wgląd do zapisanego materiału wideo (odtwarzanie lub archiwizacja za pomocą komputera). Ponadto oprogramowanie jest w stanie tworzyć tzw. rejestratory wirtualne, grupujące kamery z różnych rejestratorów fizycznych. Umożliwia to zebranie i wyświetlenie obrazów z nawet 64 kamer w jednym oknie ekranu komputerowego.

Jeżeli to nie wystarcza, można otworzyć kolejne, niezależne okna (maks. osiem), umożliwiające podgląd obrazu z innych kamer/rejestratorów. Posiadając stanowisko wielomonitorowe, użytkownik jest w stanie stworzyć rozbudowane centrum dozoru. To samo oprogramowanie służy do obsługi także innych modeli urządzeń z serii PDR.

Tworzenie centrum monitorowania ułatwia funkcja e-map, która jest przeznaczona do zarządzania większą instalacją CCTV, bazując na graficznej reprezentacji systemu/obiektu.

Oprócz standardowej, zdalnej obsługi możliwy jest dostęp do rejestratora z platform mobilnych, takich jak PDA lub telefon komórkowy. Ten rodzaj dostępu pozwala uzyskać obrazy wyświetlane na żywo oraz sterować kamerami obrotowymi.

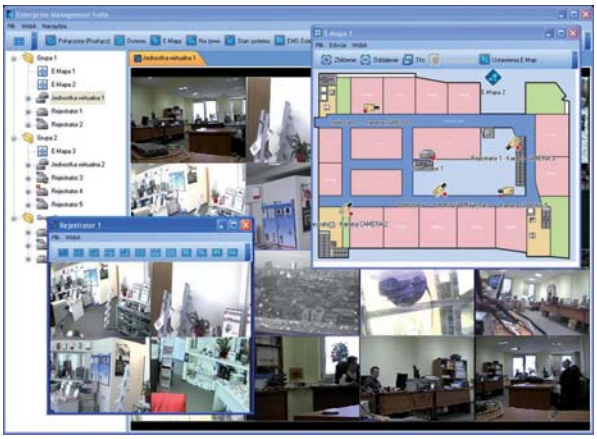
Dostęp do rejestratora jest chroniony hasłem. Urządzenie posiada jedno konto administratora, zapewniające pełne uprawnienia i pięć kont użytkowników, których uprawnienia mogą być definiowane niezależnie od siebie. Przydzielanie/odbieranie użytkownikom przywilejów, takich jak wyświetlanie obrazu w czasie rzeczywistym, odtwarzanie, archiwizacja, możliwość konfiguracji, wyłączenia rejestracji, wyłączenia urządzenia czy połączenia zdalnego przez sieć, pozostaje w gestii administratora.

PDR-XM stosuje najpopularniejszą obecnie metodę kompresji – H.264, która w dziedzinie CCTV jest najbardziej uniwersalnym sposobem komprymacji materiału wideo. Pozwala ona uzyskać dużo mniejszy strumień/rozmiar klatki w porównaniu z metodami JPEG czy MPEG. Dzięki temu następuje ograniczenie przestrzeni zajmowanej przez nagrania na dyskach twardych oraz zmniejszenie wymagań dotyczących pasma sieciowego, co pociąga za sobą zmniejszenie związanych z tym kosztów.

Rejestracja obrazu jest dokonywana na wewnętrznym dysku SATA. Obecnie obsługiwana pojemność nośnika wynosi 2 TB, niemniej PDR-XM nie wyklucza stosowania dysków o większych rozmiarach. W przypadku pojawienia się na rynku takich nośników będzie możliwe ich zastosowanie.

Dopasowanie do warunków pracy w monitorowanym obiekcie ułatwiają rozmaite tryby rejestracji: ciągłej lub zgodnej z harmonogramem, w wyniku detekcji ruchu i w wyniku alarmu (w trybie prealarmowym i postalarmowym). Jeżeli system CCTV nie wymaga nieprzerwanego zapisu obrazu, można znacznie zaoszczędzić pamięć dyskową.

Archiwizacja, podobnie jak rejestracja, może być wykonywana lokalnie lub zdalnie, w oparciu o sieć IP, za pomocą oprogramowania klienckiego. Podczas kopiowania nagrań na lokalnym



Fot. 3. Oprogramowanie Aper EMS – tryb „multiwindow”

Fot. 4. Oprogramowanie Aper EMS – tryb „multicamera”

nośniku USB Flash (*pendrive*) wraz z właściwym materiałem wizyjnym rejestrator automatycznie udostępnia aplikację odtwarzającą. Użytkownik nie musi instalować na komputerze dodatkowego oprogramowania w celu odtworzenia archiwum.

Głównym zadaniem rejestratora jest oczywiście nagrywanie obrazu (i dźwięku), PDR-XM jest jednak w stanie dokonywać również akwizycji informacji o ważnych zdarzeniach (wykonywanych działaniach, sytuacjach alarmowych) odnotowanych przez urządzenie. Dane te są zapisywane w dzienniku zdarzeń i – w połączeniu z materiałem wizyjnym – stanowią cenne źródło informacji na temat dozorowanego obiektu. Ponadto komunikaty dotyczące najistotniejszych zdarzeń, takich jak sygnał na wejściu alarmowym, detekcja ruchu, utrata sygnału wizji, awaria dysku itp., mogą być wysyłane pocztą elektroniczną na podany adres e-mailowy. Te dane są też na bieżąco wyświetlane przez oprogramowanie sieciowe. Wizualizacja zdarzeń alarmowych pozwala łatwo kontrolować stan całego systemu i poszczególnych rejestratorów wchodzących w jego skład. Pracę większej instalacji CCTV ułatwia opcja synchronizacji czasu.

Fot. 5. Aplikacja Aper PDAViewer

Ogromną zaletą rejestratorów PDR-XM jest kompatybilność z innymi urządzeniami Aper serii PDR oraz oprogramowaniem sieciowym przeznaczonym do ich obsługi. Zgodność ta wynika z faktu, iż obecnie wszystkie rejestratory PDR mają zbliżone możliwości konfiguracyjne. Zatem ustawienia, opcje i funkcjonalność PDR-XM dorównują wyższym modelom rejestratorów Aper, takim jak PDR-M czy PDR-X, a różnica dotyczy szybkości rejestracji, wydajności pracy sieciowej i liczby obsługiwanych dysków. Dzięki temu PDR-XM znajduje zastosowanie nie tylko w małych i prostych instalacjach telewizji dozorowej. Rejestratory te mogą być z powodzeniem wykorzystane w tych fragmentach bardziej zaawansowanych systemów CCTV, w których instalowanie urządzeń o wysokich prędkościach zapisu nie znajduje uzasadnienia, a od zastosowanego rejestratora oczekuje się wydajności mieszczącej się w granicach rozsądku, przy zachowaniu dobrej jakości i funkcjonalności.

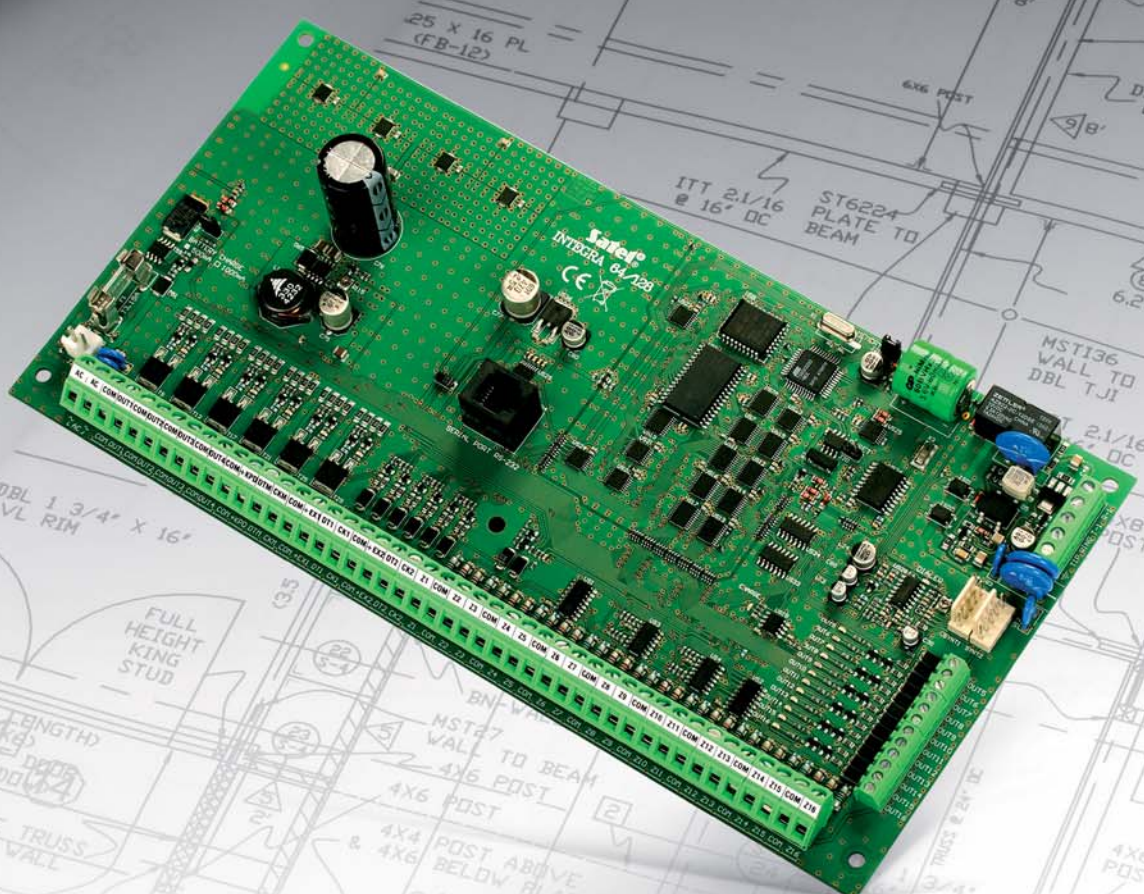
Mariusz Witulski
S.P.S. Trading

Fot. 6. PDR-XM3008 – panel przedni (u góry) – panel tylny (na dole)

Integra
więcej niż bezpieczeństwo

Niezawodność i zaawansowana funkcjonalność wykraczająca poza zastosowania alarmowe. Jeden system łączący ochronę mienia i automatykę w inteligentny system zarządzania obiektem.

Idealne rozwiązanie do mieszkań, dla domów jednorodzinnych, jak i budynków użyteczności publicznej.



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

Realne koszty systemu wykrywania pożaru

Kilka ważnych uwag

Grzegorz Ćwiek

W ciągu ostatnich dwudziestu lat w systemy sygnalizacji pożarowej wyposażono w Polsce niezliczoną ilość rozmaitych obiektów – małe kamienice adaptowane na biurowce i hotele, profesjonalne centra biurowe i handlowe, obiekty zabytkowe, sakralne i wreszcie, ostatnio, ogromne obiekty sportowo-rekreacyjne. W wielu miejscach przyjęte dla takich obiektów zasady bezpieczeństwa i koncepcje zabezpieczeń wydają się być optymalne – zarówno pod względem technicznym, jak i cenowym. Ale czy tak jest na pewno? Czy pieniądze wydatkowane na system bezpieczeństwa to pieniądze wydane właściwie czy nie? Czy cena jest adekwatna do wartości zastosowanego zabezpieczenia? Czy wreszcie koszt, który poniesiono w fazie inwestycji, jest kosztem ostatecznym?

W niniejszym artykule nie będziemy zajmować się fazą początkową, a więc kosztami samego przygotowania projektu, choć implikacje tej fazy dla wartości całości inwestycji są ogromne. Czasem mają one istotne konsekwencje dla właścicieli – szczególnie, gdy w fazie tej zostaną popełnione błędy. Jest to jednak na tyle szerokie zagadnienie, że moglibyśmy poświęcić mu wiele stron osobnego artykułu, dlatego teraz nie będziemy się nim zajmować.

Chciałbym zwrócić uwagę przede wszystkim na dodatkowe koszty systemu sygnalizacji pożarowej, które mogą i zwykle pojawiają się już po jego kupieniu i zainstalowaniu w obiekcie, a zatem w momencie, gdy źle przygotowana inwestycja zostaje uznana za zakończoną, a pozornie niskie koszty całkowite systemu, błędnie ocenione np. w fazie przetargowej, zaczynają dramatycznie rosnąć, powodując dalsze utrudnienia dla wszystkich uczestników projektu – także osób postronnych, a więc przyszłych najemców i innych osób odwiedzających budynek w trakcie jego eksploatacji. Zresztą do tej sprawy wrócimy jeszcze pod koniec niniejszego artykułu.

Instalacje i systemy oszczędne, ale bez możliwości rozwoju i adaptacji

Jeszcze kilkanaście lat temu prawo nakładające na właścicieli i administratorów obiektów obowiązek instalowania podobnych systemów było nieco bardziej liberalne lub – inaczej – mniej precyzyjne niż dzisiaj. Zakres zastosowania systemów automatycznej detekcji pożaru był określony przez wytyczne i standardy zapożyczone z krajów zachodnich, najczęściej zmodyfikowane według lokalnie przyjętych, bardziej lub mniej wytłumaczalnych zasad. Oczywiście nie można tu nikogo winić; dwadzieścia czy nawet piętnaście lat temu – mimo braku konkretnych przepisów, dzięki potężnemu zaangażowaniu całego grona entuzjastów i ówczesnych ekspertów – zaszły zmiany w tym zakresie i zastosowano rozwiązania, które z pewnością ograniczyły straty materialne i uratowały wiele istnień ludzkich przed zagrożeniem. Ważną rolę odegrali tu sami producenci tego typu rozwiązań, kreując na nowo kulturę techniczną w tej dziedzinie. Nie wolno zapominać o polskich pionierach, takich jak przedstawiciele ówczesnej Państwowej Straży Pożarnej czy pracownicy instytutów badawczych i naukowych. Niestety zbyt mały udział mieli (i nadal mają!) w tym wszystkim w Polsce ubezpieczyciele – za wyjątkiem niektórych przedsiębiorstw i przedstawicielstw koncernów zagranicznych, które, czerpiąc z doświadczeń ich rodzimych rynków, były i nadal są w stanie lepiej rozumieć istotę problemu.

Na przestrzeni lat przepisy stały się bardziej precyzyjne, w wielu miejscach zaostrzono je zdecydowanie, a ponadto wprowadzono szereg zmian skutkujących pojawieniem się w obiektach dodatkowych elementów lub systemów bezpieczeństwa, których współdziałanie jest ściśle związane z systemem SAP (np. dźwiękowych systemów ostrzegawczych – DSO). Okazało się, że niektóre instalacje już po kilku latach – na skutek zmian w przepisach i normach – muszą zostać zmodernizowane. Dochodzimy do pierwszego ważnego spostrzeżenia: **realny koszt systemu sygnalizacji pożarowej – nawet po kilku latach od momentu jego zainstalowania – może znacznie zwiększyć się na skutek zmian w przepisach.** Pomijając okres, w którym następuje dostosowanie się do nowych przepisów i który może przynieść inwestorowi chwilową ulgę, koszt takiej modernizacji może wynieść od kilkudziesięciu do prawie 200% wartości nowo zainstalowanego systemu! Tak ogromny koszt wiąże się z koniecznością przebudowy infrastruktury kablowej i komunikacyjnej, koniecznością pracy ekip w warunkach funkcjonującego (oddanego do użytku) obiektu (najczęściej nocą, gdy stawki za roboczogodzinę są znacznie większe), a nawet z koniecznością utylizacji elementów już zainstalowanych i zastąpieniem ich innymi urządzeniami. Znane są przypadki z lat 90., czyli z okresu istotnych zmian w obowiązujących przepisach, kiedy to w ciągu dwóch lat trzeba było zwiększyć liczbę zastosowanych detektorów i innych elementów peryferyjnych systemu o prawie 50%. W rezultacie konieczna stała się wymiana całego systemu sygnalizacji pożarowej, gdyż nie można było tak znacznie rozbudować taniego systemu, skrojonego wcześniej na miarę.

Od fazy projektowej do uruchomienia obiektu – dostosowanie systemu do rzeczywistych zadań w obiekcie

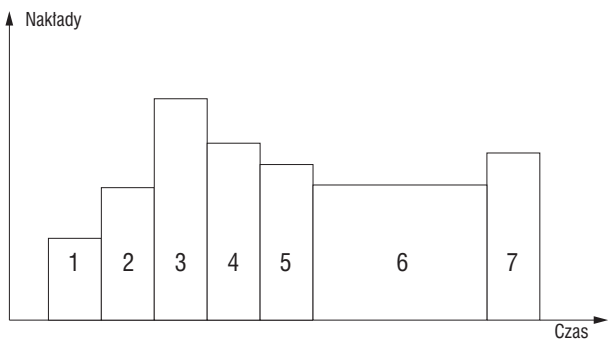
Kolejnym istotnym kosztem, z którego nadal niewielu inwestorów zdaje sobie sprawę, jest **koszt użytkowania systemu tuż po jego zainstalowaniu** w obiekcie i odbiorze budynku, a raczej potencjalnego braku możliwości jego użytkowania w tej fazie inwestycji. To brzmi nieco dziwnie i być może mało realistycznie, ale za chwilę udowodnię tę tezę. Dochodzimy tutaj do ujawnienia pewnej znanej wszystkim tajemnicy branżowej. Oczywiście skala tego zjawiska bywa różna i w wielu przypadkach dodatkowe koszty występujące w tej fazie nie muszą być duże. Zależy to od rzetelności wszystkich – dosłownie wszystkich uczestników realizowanego projektu.

Instalacje niskoprądowe najczęściej są wykonywane w dużym pośpiechu i w warunkach znacznych opóźnień budowy. Do tego należy dodać dokonywane w trakcie realizacji zmiany w koncepcji lub projekcie lub zamiany jednych systemów na drugie i odwrotnie. Rezultatem takiego „zwykłego" zamieszania jest najczęściej utrata kontroli wszystkich uczestników projektu nad prawidłowością wdrożenia systemu bezpieczeństwa pożarowego z punktu widzenia zadań, jakie miał on realizować według początkowych założeń. Inaczej mówiąc – zmianom w scenariuszu rozwoju zdarzeń, sprzęcie, projekcie wykonawczym, przyjętych odstępstwach, matrycy sterowań itd. nie towarzyszy (lub w niewystarczający sposób odpowiada) korekta interakcji pomiędzy wszystkimi elementami techniczno-funkcjonalnymi instalacji. Dochodzi do sytuacji, w której nie ma czasu i możliwości ponownego, spokojnego przeanalizowania wszystkich zmian, nie tylko w ramach jednej instalacji: całkowicie niewydolna okazuje się koordynacja zadań na styku wielu branż. Skutkiem tego odebrany zostaje system działający poprawnie z punktu widzenia technicznego i zwykle realizujący podstawowe zadania związane z bezpieczeństwem przeciwpożarowym obiektu, ale – w ujęciu realnym – nie funkcjonujący w taki sposób, jaki zakładano w założeniach projektowych. Odbierający system i wydający pozwolenia na użytkowanie nie są bowiem w stanie, przy całym swym zaangażowaniu i dobrej woli, w pełni przewidzieć ostatecznej skuteczności systemu.

Najczęściej już po odebraniu instalacji i wydaniu pozwolenia na użytkowanie obiektu następuje trwająca około jednego roku niezwykle kosztowna faza weryfikacji przyjętych założeń, zmian w oprogramowaniu, scenariuszu i matrycy sterowań elementami automatyki pożarowej itd. Koszt pracy inżynierów ekspertów i rzeczoznawców rozkłada się tu w różnych proporcjach

pomiędzy właściciela obiektu, instalatorów i nadzór związany z zarządzaniem obiektem. Koszty te, w zależności od stopnia zaniedbań we wszystkich poprzednich fazach realizacji projektu, wynoszą od kilku do kilkudziesięciu procent wartości inwestycji. Ze względu na nieprzewidziane wcześniej zmiany funkcjonalności obiektu nawet w przypadkach bardzo dobrze prowadzonych i koordynowanych projektów faza dostosowawcza systemu generuje dodatkowy koszt wynoszący do kilkunastu procent wartości ceny przetargowej.

Poniższy diagram obrazuje przebieg realizacji podobnego projektu w odniesieniu do nakładów ponoszonych w czasie:



1. Analiza zagrożeń i opracowanie założeń wstępnych
2. Koncepcja zabezpieczeń i podstawowe uzgodnienia, projekty wstępne
3. Definicja projektu, dobór urządzeń i podstawowego zakresu sterowań, koordynacja
4. Dalsze prace adaptacyjne, początek fazy wykonawczej
5. Faza wykonawcza – ciąg dalszy realizacji, aż do oddania obiektu
6. Adaptacja systemu po odebraniu instalacji; koszt utrzymania systemu, serwis, okresowe przeglądy
7. Wycofanie z użytkowania

Z powyższego diagramu wynika bardzo jasno, że wstępna faza przygotowania prawidłowej koncepcji i projektu oraz dobór urządzeń powinny odpowiadać istotnej części nakładów finansowych i osobowych, a także zajmować odpowiednią ilość czasu po to, by maksymalnie zredukować koszty samego wykonania instalacji i jej utrzymania w późniejszym czasie. Im rzetelniej wykonany jest projekt, im wyższego rzędu wiedza inżynierska zostanie wykorzystana w tej fazie inwestycji, tym niższy jest realny koszt zakupionego systemu bezpieczeństwa. Można powiedzieć, że realny koszt tej i innych podobnych instalacji zależy od stopnia kultury technicznej i rozsądku każdego z uczestników projektu w każdej fazie – od fazy koncepcji, w której bierze się pod uwagę przyszłe, możliwe zmiany prawne (niektóre nietrudno przewidzieć) i rozwój funkcjonalności obiektu, a także dobiera sprzęt o odpowiednich parametrach technicznych i możliwościach rozwojowych (szeroka przestrzeń adresowa, możliwość sieciowania, kompatybilność wstecz itd.), poprzez fazę uzgodnień i koordynacji międzybranżowych, w której należy przewidzieć wszelkie możliwe sposoby interakcji różnych współistniejących systemów, aż po fazę końcową, w której nadaje się systemowi ostateczny kształt – przy czym należy zdawać sobie sprawę, że system bezpieczeństwa z natury rzeczy nigdy nie osiąga kształtu ostatecznego. Musi „żyć" razem z obiektem, a koszty związane z dostosowywaniem go do zmian w otoczeniu muszą być brane pod uwagę już w fazie wyboru producenta, dostawcy oraz instalatora. Będzie miało to istotny wpływ na wieloletnie wydatki właściciela i bezpieczeństwo użytkowników obiektu.

Grzegorz Ćwiek

ZAKOPYWANE SYSTEMY OCHRONY OBWODOWEJ

więcej na: **www.atline.pl**

firma ATLine®
kompleksowe zabezpieczanie obiektów

PPS

GPS Plus

Panther II

Omnitrax

PROJEKTOWANIE KOMPLEKSOWYCH DOKUMENTACJI

- technicznych, architektoniczno - budowlanych wraz z niezbędnymi branżami specjalistycznymi obiektów biurowych i przemysłowych
- innowacyjnych systemów ochrony
- teletechnicznych, elektrycznych i automatyki przemysłowej

WYKONAWSTWO

zaawansowanych technologicznie systemów ochrony i bezpieczeństwa

SPRZEDAŻ

nowoczesnych systemów ochrony

Firma ATLine sp.j. Sławomir Pruski
ul. Franciszkańska 125, 91-845 Łódź
tel. +48 042 657 30 80, fax +48 042 655 20 99
e-mail: info@atline.pl, handel@atline.pl

ZSJZ

AQAP 2110:2006

Konwencjonalny system sygnalizacji pożarowej IGNIS 1000

Krzysztof Marchlewski

Konwencjonalny system sygnalizacji pożarowej IGNIS 1000 jest stosowany w instalacjach sygnalizacji pożaru w małych i średnich obiektach. Jest on chętnie instalowany pomimo coraz powszechniejszego wykorzystywania systemów adresowalnych, a to dzięki nowoczesnej konstrukcji urządzeń tworzących system, bogatej ofercie tych urządzeń i ich rozsądnej cenie. IGNIS 1000 służy do budowy systemów ochrony przeciwpożarowej w różnych obiektach, np. w magazynach, biurach, hurtowniach, domach mieszkalnych, obiektach o dużym znaczeniu strategicznym (np. w wyniesionych centralach telefonicznych), jak i zabytkowych (np. w budowlach sakralnych). Nadaje się także do ochrony przeciwpożarowej budynków i pomieszczeń położonych na terenie jednostek wojskowych, takich jak magazyny broni, pomieszczenia komputerowe, kancelarie, archiwa. Może także pracować jako wyniesiona instalacja sygnalizacji pożarowej w systemach hierarchicznych

Urządzenia tworzące system IGNIS 1000

System składa się z następujących urządzeń:

1) centrale sygnalizacji pożarowej:
   – IGNIS 1030 o 3 liniach dozorowych,
   – IGNIS 1080 o 8 liniach dozorowych,
   – IGNIS 1240 o 16 liniach dozorowych z możliwością rozbudowy do 24 linii,
   – IGNIS 1520M – centrala sterowania urządzeniami gaśniczymi;
2) konwencjonalne czujki pożarowe szeregu 40 (instalowane w gniazdach G-40):
   – uniwersalna optyczna czujka dymu DUR-40,
   – standardowa optyczna czujka dymu DOR-40,
   – jonizacyjna czujka dymu DIO-40,
   – wielodetektorowa czujka DOT-40,
   – wielodetektorowa czujka TOP-40,
   – czujka ciepła TUP-40,
   – liniowa czujka dymu DOP-40 (nie wymaga gniazda);
3) czujki w wykonaniu iskrobezpiecznym:
   – optyczna czujka dymu DUR-40Ex (wymaga gniazda G-40),
   – jonizacyjna czujka dymu DIO-37Ex (wymaga gniazda G-33),
   – czujka płomienia PUO-35Ex (dostępna jest także czujka PUO-35 w wykonaniu zwykłym do powszechnych zastosowań; czujki wymagają gniazda G-33),
   – uniwersalna czujka ciepła TUN-38Ex (nie wymaga gniazda);
4) ręczne ostrzegacze pożarowe ROP-63 i ROP-63H;
5) wskaźniki zadziałania WZ-31;
6) tablica alarmowa TW-35.

Centrale systemu IGNIS 1000

W ramach systemu dostępne są centrale mające od trzech do 24 linii dozorowych oraz wyspecjalizowana centrala sterująca automatycznymi urządzeniami gaśniczymi IGNIS 1520M. Dobierając urządzenia do obiektu, który mamy zabezpieczyć, powinniśmy kierować się następującymi kryteriami:

– wielkością zabezpieczanego obiektu i liczbą niezbędnych do jego zabezpieczenia czujek pożarowych (tab. 1.),
– rozkładem pomieszczeń w budynku i możliwością ich łatwej identyfikacji.

W rzeczywistości liczba współpracujących z poszczególnymi centralami czujek może być większa niż liczba podana w tabeli 1, jednak, dobierając urządzenia, należy brać pod uwagę potrzebę pozostawienia rezerwy na wypadek ewentualnych zmian w instalacji (np. rozbudowy w przyszłości) oraz łatwość położenia instalacji i skonfigurowania systemu, gdy pojemność nie jest wykorzystywana maksymalnie.

Na każdej linii dozorowej (w każdej strefie) centrali można zainstalować do 32 czujek pożarowych, jedną liniową czujkę dymu DOP-40 lub do 10 ręcznych ostrzegaczy. Linie dozorowe są kontrolowane na wypadek ich uszkodzenia (przerwa, zwarcie), co wymaga zainstalowania rezystora końcowego w ostatnim elemencie linii. Sygnalizując alarm pożarowy lub uszkodzenie, centrala wskazuje numer linii dozorowej, na której ma miejsce dane zdarzenie. Linia dozorowa może objąć tylko jedną strefę pożarową o powierzchni do 1600 m^2. Ponieważ w konwencjonalnym systemie identyfikacja miejsca alarmu odbywa się przez wskazanie linii dozorowej z alarmującą czujką, nie jest możliwe precyzyjne określenie pomieszczenia, w którym zainstalowano czujkę, jeżeli linia dozorowa obejmuje kilka pomieszczeń. Aby zidentyfikować pomieszczenie, należy zastosować wskaźniki zadziałania WZ-31 zainstalowane nad drzwiami do pomieszczeń.

Cechy funkcjonalne i wyposażenie central IGNIS 1030, 1080 i 1240:

1) 3, 8, 16 lub 24 linie dozorowe (strefy),
2) linia do zasilania i sterowania zewnętrznymi sygnalizatorami,
3) linie kontrolne do nadzorowania dołączonych dodatkowych urządzeń zewnętrznych,
4) wyjście (wbudowany interfejs) do podłączenia tablicy alarmowej TW-35 przeznaczonej do powielenia głównych sygnałów centrali w oddalonym miejscu (tylko dla central IGNIS 1080 i IGNIS 1240),
5) interfejs szeregowy RS232 umożliwiający przesłanie zdarzeń pamiętanych przez centralę do komputera PC,
6) wyjścia przekaźnikowe alarmu ogólnego z możliwością ustawienia opóźnienia zadziałania,

Typ centrali	Zalecane zastosowanie
IGNIS 1030	Małe budynki o maksymalnie 2 kondygnacjach, wymagające zabezpieczenia do 10 pomieszczeń przez maksymalnie 20 czujek
IGNIS 1080	Małe budynki o maksymalnie 6 kondygnacjach, wymagające zabezpieczenia do 30 pomieszczeń przez maksymalnie 50 czujek
IGNIS 1240	Średnie budynki o maksymalnie 10 kondygnacjach, wymagające zabezpieczenia do 100 pomieszczeń przez maksymalnie 200 czujek
IGNIS 1520M	Uruchamianie jednostrefowych stałych urządzeń gaśniczych, głównie gazowych, w archiwach, serwerowniach, pomieszczeniach automatyki itp.

Tab. 1. Zakres szacunkowy stosowania central systemu IGNIS 1000

7) wyjście przekaźnikowe uszkodzenia ogólnego,
8) wyjście przekaźnikowe z każdej linii dozorowej do sterowania urządzeniami zewnętrznymi, z możliwością programowania zadziałania według kryterium alarmu z jednej lub dowolnej liczby stref,
9) wyjście do zasilania urządzeń zewnętrznych,
10) zasilacz sieciowy z automatycznym ładowaniem rezerwowej baterii akumulatorów,
11) wewnętrzna bateria akumulatorów do zasilania rezerwowego przez 72 h,
12) ciągła kontrola baterii z automatycznym odłączeniem i sygnalizacją jej rozładowania,
13) zegar czasu rzeczywistego,
14) pamięć 512 zdarzeń,
15) licznik alarmów pożarowych – maksymalnie 9999 alarmów,
16) możliwość zaprogramowania różnych wariantów alarmowania:
– jednostopniowe lub dwustopniowe zwykłe,
– jednostopniowe lub dwustopniowe ze wstępnym kasowaniem,
– jednostopniowe lub dwustopniowe ze współzależnością strefowo-czasową,
17) programowanie pracy centrali w trybie obsługa obecna/brak obsługi,
18) ciągła kontrola sprawności linii dozorowych, sygnałowych i kontrolnych dotycząca wystąpienia przerwy, zwarcia i doziemienia,
19) możliwość blokowania wyjść do sterowania monitorowaniem i sygnalizatorami akustycznymi,
20) możliwość wyłączania linii dozorowych,
21) możliwość testowania elementów sygnalizacyjnych i czujek na liniach dozorowych,
22) trzy poziomy dostępu do elementów obsługowych centrali, w tym dostęp z użyciem klucza,
23) sygnalizacja ogólna „POŻAR” ze wskazaniem strefy (linii), w której powstał pożar,
24) sygnalizacja ogólna „USZKODZENIE” ze wskazaniem uszkodzonej linii z czujkami oraz możliwość identyfikacji każdego uszkodzenia: systemowego, zasilania, sygnalizatorów, dodatkowych urządzeń zewnętrznych, doziemienia,
25) komunikatywne opisy i funkcjonalne elementy obsługowe,
26) małe wymiary (wraz z wewnętrzną baterią zasilania rezerwowego).

Konwencjonalne czujki pożarowe

O skuteczności działania konwencjonalnego systemu sygnalizacji pożarowej decydują w głównej mierze czujki pożarowe i właściwy dobór tych czujek do rodzaju chronionego obiektu. Czujki szeregu 40 są czujkami dwustanowymi, tzn. mogą pracować w dwóch trybach: dozorowania i alarmu pożarowego. Decyzja o wysłaniu do centrali sygnału alarmu pożarowego jest podejmowana przez układ procesorowy czujek po wykryciu obecności, obróbce i weryfikacji czynnika pożarowego. Dalsza weryfikacja sygnału alarmu pożarowego może być dokonana przez współpracującą centralę, w której możliwe jest ustawienie wielu różnych wariantów alarmowania m. in. wstępnego kasowania sygnału czujki, alarmowania dwustopniowego, koincydencji dwóch stref dozorowych itd. Czujki mają także wbudowane układy

Parametr	DUR-40	DOR-40	DIO-40	DOT-40	TOP-40	TUP-40	DOP-40
Zastosowany sensor (detektor)	Optyczny rozproszeniowy	Optyczny rozproszeniowy	Komora jonizacyjna	Optyczny rozproszeniowy + cieplny	Cieplny + płomieniowy IR	Cieplny	Optyczny absorpcyjny
Maks. prąd dozorowania	60 μA	60 μA	60 μA	60 μA	90 μA	40 μA	5 mA / 2,2 mA
Wykrywane pożary testowe	Od TF1 do TF5 oraz TF8	Od TF2 do TF5	Od TF1 do TF5 oraz TF8	Od TF1 do TF6 oraz TF8	TF1, od TF4 do TF6	nie bada się	Od TF1 do TF5
Klasa detektora ciepła	–	–	–	A1	A1R	A1R	–
Tryb pracy/ czułość (do wyboru)	–	–	–	DOR i TUP DOR TUP	TUP wspomagany przez IR	–	18% – cz. duża 30% – cz. średnia 50% – cz. mała
Kąt widzenia sensora płomienia/zasięg	–	–	–	–	60° klasa 2 (17 m)	–	czujka – reflektor 5 ÷ 100 m
Maks. wysokość instalowania	11 m	11 m	11 m	8 m lub 11 m w trybie DOR	8 m	8 m	11 m lub 25 m przy dwóch poziomach czujek

Tab. 2. Zestawienie czujek konwencjonalnych szeregu 40

automatycznej kompensacji czułości, tzn. utrzymują stałą czułość przy postępującym zabrudzeniu komór pomiarowych oraz przy zmianach wilgotności i temperatury środowiska, w którym pracują.

W tabeli 2 podano istotne dla projektanta i instalatora parametry podstawowych czujek konwencjonalnych.

Optyczne czujki dymu DUR i DOR różnią się rodzajem zastosowanych diod nadawczych w układzie optycznym i w związku z tym emitowanym promieniowaniem, rozpraszanym na cząsteczkach dymu. Czujka DUR wykorzystuje promieniowanie o krótszej fali niż czujka DOR oraz DOT.

Charakterystyki wybranych czujek konwencjonalnych

Liniowa czujka dymu DOP-40

Czujka DOP-40 jest przeznaczona do ochrony zwłaszcza takich pomieszczeń, w których ze względu na dużą powierzchnię należałoby zastosować bardzo dużą liczbę punktowych czujek dymu, a także pomieszczeń, w których z różnych względów nie można zainstalować czujek punktowych. Czujka analizuje średnią wartość gęstości dymu na drodze wiązki wysyłanego promieniowania podczerwonego, a zatem jest szczególnie przydatna, gdzie dym może ulec rozproszeniu na dużym obszarze przed detekcją. Przykładowe obiekty, które są predysponowane do zainstalowania tego typu czujek, to: kościoły, katedry, obiekty zabytkowe ze stropami o dużej wartości historycznej, teatry, opery, hale widowiskowe, hale produkcyjne, bardzo wysokie pomieszczenia, w których czujki punktowe byłyby nieskuteczne, pomieszczenia o zróżnicowanej budowie stropu, korytarze, kanały kablowe, przestrzenie nad podwieszanymi sufitami itp.

Nadajnik i odbiornik czujki DOP-40 są zintegrowane w jednej obudowie. Wysyłana przez nadajnik czujki wiązka podczerwieni odbija się od specjalnego reflektora pryzmowego (lub zespołu reflektorów) i powraca do odbiornika. W takiej konstrukcji nie trzeba łączyć kablem nadajnika i odbiornika w celu synchronizacji ich pracy, dlatego znacznie zmniejsza się koszt instalacji. Czujka ma wbudowany celownik laserowy, pozwalający na łatwe i precyzyjne zestrojenie toru optycznego czujki, co jest czynnością bardzo pracochłonną, zwłaszcza przy dużych odległościach. Specjalny reflektor pryzmowy posiada dodatkową zdolność skupiania wiązki optycznej czujki i kierowania jej do nadajnika. Umożliwia to instalowanie reflektorów na ścianach i konstrukcjach podlegających niewielkim drganiom, np. wynikającym z pracy zainstalowanych ciężkich maszyn, jak również odkształceniom w wyniku dużych zmian temperatury (np. między dniem a nocą). Czujka analizuje chronioną przestrzeń i po kilkukrotnej weryfikacji wartości mierzonej i porównaniu jej z różnymi modelami rozwoju pożaru podejmuje decyzję o stanie alarmu pożarowego. Ze względu na zdolność samoregulacji odpowiednio wcześnie zgłasza obsłudze fakt zabrudzenia swojego układu optycznego (np. osadzenia się na nim kurzu), a jednocześnie zachowuje zdolność wykrywania zagrożenia pożarowego. Praktycznie płaska charakterystyka czułości, niezależna od wielkości cząstek dymu (aerozolu), stwarza możliwość jej wszechstronnego zastosowania. Możliwość ustawiania różnych

progów czułości działania w zależności od odległości pomiędzy czujką a lustrem/reflektorem oraz od warunków środowiskowych pozwala na doskonałe dopasowanie jej do różnych środowisk pracy. Czujka może chronić do 1200 m^2 powierzchni, czyli tyle, ile kilkanaście punktowych czujek dymu przy możliwych większych wysokościach instalowania, a niewielki pobór prądu umożliwia pracę wielu czujek w instalacjach z jedną centralą. Produkowana jest również wersja DOP-40R, wyposażona w przekaźniki wyjściowe, które pozwalają na dołączenie jej do dowolnej centrali innych producentów.

Wielodetektorowa czujka dymu i ciepła DOT-40

Czujka DOT-40 wykrywa pożary, którym towarzyszy dym i (lub) wzrost temperatury. Zawiera dwa detektory – klasyczny rozproszeniowy detektor dymu i termistorowy detektor ciepła – z których sygnały są poddawane zaawansowanej analizie sygnałowej przez mikroprocesor podejmujący decyzje o zadziałaniu czujki. Czujka charakteryzuje się znaczną odpornością na ruch powietrza i zmiany ciśnienia. Ponieważ detektor ciepła wykrywa pożar z niższej wysokości niż detektor dymu, można ją instalować jako czujkę dualną na wysokości do ośmiu metrów. Powyżej tej wysokości działać będzie tylko detektor dymu. W szczególnych przypadkach, gdy zależy nam na jednorodności instalowanych czujek, czujkę DOT-40 można wykorzystać albo jako czujkę dymu typu DOR-40 albo jako czujkę ciepła typu TUP-40, odpowiednio przekładając zworę w programatorze czujki.

Ze względu na swoje cechy, czujka szczególnie nadaje się do zabezpieczania garaży.

Wielodetektorowa czujka ciepła i płomienia TOP-40

Czujka TOP-40 wykrywa pożary, którym towarzyszy płomień i (lub) wzrost temperatury. Zastosowanie dwóch sensorów – ciepła i promieniowania podczerwonego – pozwala na uzyskanie zwiększonej odporności czujki na zakłócenia i minimalizuje ryzyko wystąpienia fałszywych alarmów. Informacje z sensorów płomienia i ciepła są poddawane zaawansowanej analizie przez mikrokontroler nadzorujący pracę czujki i oceniający zagrożenie pożarowe. Po wykryciu płomienia piroelement, jako sensor promieniowania IR, ma wpływ na wzrost czułości toru temperaturowego. Czujka TOP-40 jest polecana do stosowania w miejscach, gdzie ze względu na panujące warunki nie można stosować czujek dymu, a więc może być szczególnie przydatna do dozorowania pomieszczeń, w których stale lub okresowo panuje zadymienie, zapylenie itp. – klasa szczelności obudowy to IP44.

Uniwersalna czujka ciepła TUN-38Ex

Czujka TUN-38Ex jest produkowana w wykonaniu iskrobezpiecznym, ale może być również instalowana na zwykłych liniach dozorowych, gdy wymagana jest praca w trudnych warunkach środowiskowych (klasa szczelności obudowy IP44). Czujka nie wymaga gniazda montażowego i jest mocowana wkrętami bezpośrednio do stropu. Przewody wejścia i wyjścia linii dozorowej są wprowadzane przez dławnice kablowe. Obudowa jest wykonana z tworzywa, które nie gromadzi ładunków elektrycznych. Można zaprogramować różne rodzaje pracy czujki TUN-38Ex poprzez odpowiednie rozmieszczenie zworek, dostępnych po zdjęciu pokrywki osłaniającej łączówki.

Czujka może pracować w klasach:

- A1R o charakterystyce nadmiarowo-różniczkowej i maksymalnej temperaturze użytkowania do + 50°C z dwoma podklasami: A1R-L o nominalnej czułości i A1R-H o zwiększonej czułości;
- A1S o charakterystyce nadmiarowej i maksymalnej temperaturze użytkowania do + 50 °C;
- BR o charakterystyce nadmiarowo-różniczkowej i maksymalnej temperaturze użytkowania do + 65°C;
- BS o charakterystyce nadmiarowej i maksymalnej temperaturze użytkowania do + 65°C.

Podsumowanie

Urządzenia systemu IGNIS 1000 spełniają wszystkie wymagania stawiane współczesnym systemom wykrywającym i powiadamiającym o pożarze, określone w odpowiednich arkuszach normy EN 54. Mają także aktualne certyfikaty zgodności i świadectwa dopuszczenia, pozwalające na ich stosowanie w ochronie przeciwpożarowej. Ze względu na wiele zalet, takich jak wysoki poziom techniczny, niezawodność, stosunkowo niska cena, łatwość serwisowania i napraw, są bardzo chętnie stosowane przez wielu inwestorów.

Krzysztof Marchlewski
POLON-ALFA

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

POLON 4100

NOWY WYMIAR BEZPIECZEŃSTWA

„POLON-ALFA" Zakład Urządzeń Dozymetrycznych sp. z o.o.

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

ODKRYJ SZYBKOŚĆ INSTALACJI

DSC

WT5500
Bezprzewodowa klawiatura LCD

WT4989
Bezprzewodowy pilot
z wyświetlaczem LCD

WS4904W
Bezprzewodowe czujki PIR

WS4945
Bezprzewodowa
czujka kontaktronowa

Wyłączny dystrybutor produktów DSC w Polsce:

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

ALEXOR PC9155

BEZPRZEWODOWY SYSTEM ALARMOWY
O KOMUNIKACJI DWUKIERUNKOWEJ

- Obsługa maksymalnie 32 urządzeń bezprzewodowych i 16 breloków
- Kompatybilność z urządzeniami o komunikacji jednokierunkowej
- Obsługa do 4 sygnalizatorów i klawiatur bezprzewodowych
- Funkcja automatycznego przypisywania urządzeń bezprzewodowych
- Szablony programowania skracające czas instalacji
- 16 kodów użytkownika, 1 kod główny, 1 kod konserwatora
- Funkcja sprawdzania kodu identyfikacyjnego systemu
- Alternatywna komunikacja przez sieć GSM/GPRS lub TCP/IP
- Wbudowany sygnalizator akustyczny o mocy 85dB
- 2 zaciski I/O, które mogą być zaprogramowane jako wyjścia PGM lub przewodowe linie dozorowe
- 200mA obciążalności prądowej wyjścia AUX
- Rejestr 500 zdarzeń
- Podwójne zabezpieczenie antysabotażowe przed otwarciem obudowy lub oderwaniem od ściany
- 24 godzinne podtrzymanie baterii

Pozostałe urządzenia bezprzewodowe kompatybilne z centralą PC9155:

WS4939, PT4
Bezprzewodowy pilot i brelok zbliżeniowy

TL265GS, GS2065
Komunikatory alarmowe wysyłające kody raportujące przez sieć GSM/GPRS i TCP/IP

WT4901
Bezprzewodowy sygnalizator wewnętrzny

WT4911
Bezprzewodowy sygnalizator zewnętrzny

WS4916
Bezprzewodowa czujka dymu

WS4985
Bezprzewodowa czujka zalania wodą

WLS912L
Bezprzewodowa czujka zbicia szyby

WS4975
Bezprzewodowa czujka kontaktronowa

Fot. 1. PX200N

PX200N OSM.2007 Para na medal

System transmisji alarmu wykorzystujący nadajnik PX200N z redundantnym Odbiornikiem Systemu Monitoringu OSM.2007 uzyskał pierwszą nagrodę w konkursie „Polski Mistrz Techniki Alarmowej 2010" w kategorii „urządzenia i systemy transmisji alarmu oraz monitoringu"

EBS

Produkowane przez EBS urządzenia – nadajnik PX200N i odbiornik OSM.2007 – zostały nagrodzone przez kapitułę konkursu z uwagi na ich innowacyjne funkcje, a także długą listę korzyści, jakie oferują użytkownikom.

Korzyści związane ze stosowaniem nadajnika PX200N

Wygoda

Podstawowym przeznaczeniem nadajników PX200N jest transmisja sygnałów z systemów zabezpieczeń w kanałach GPRS, SMS i PSTN. Urządzenia zostały zaprojektowane tak, aby wszyscy, którzy mają styczność z systemem zabezpieczeń – instalatorzy, operatorzy stacji monitorowania i użytkownicy końcowi (właściciele lub zarządcy monitorowanych obiektów) – mieli jak najwyższy komfort korzystania z tych urządzeń.

Nadajniki zostały wyposażone w funkcję o nazwie „monitor zdarzeń" – graficzny interfejs, który pokazuje stan danego nadajnika (czy jest podłączony, czy odbiera sygnał GPRS, jak silny jest sygnał i wiele innych informacji). Ta funkcja bardzo ułatwia pracę instalatorom, zarówno podczas zapoznawania się z urządzeniem, jak i wtedy, gdy w trakcie normalnej eksploatacji pojawią się jakiekolwiek kłopoty. Jeżeli wystąpią nieprawidłowości w trakcie pracy urządzenia, można wykorzystać funkcję „historia zdarzeń". Możliwość zdalnego wglądu w historię zdarzeń często pozwala znaleźć przyczynę pojawienia się nieprawidłowości w pracy systemu bez konieczności wyjazdu do monitorowanego obiektu.

Z myślą o wygodzie pracy instalatorów nadajniki PX200N wyposażono w złącze śrubowe z windą – element, który, dzięki swojej konstrukcji, ułatwia instalatorom mechaniczne połączenie nadajnika z innymi urządzeniami. Istotnym udogodnieniem jest możliwość zdalnej konfiguracji nadajników za pośrednictwem SMS, GPRS lub CSD, a także możliwość zdalnej aktualizacji firmware'u poprzez GPRS lub CSD. Dzięki zastosowaniu tych funkcji w nadajnikach PX200N instalatorzy nie muszą za każdym razem wyjeżdżać do monitorowanego obiektu celem skonfigurowania nadajnika lub aktualizacji jego oprogramowania wbudowanego. Nadajniki są fizycznie najbardziej oddalonymi elementami systemu transmisji alarmów, więc właściwość ta pozwala zaoszczędzić wiele czasu i pieniędzy.

Podczas projektowania nadajnika PX200N konstruktorzy EBS uwzględnili również potrzeby końcowych użytkowników urządzeń, czyli właścicieli i zarządców monitorowanych obiektów. Nadajniki PX200N umożliwiają wysyłanie sygnałów SMS o dowolnej, programowalnej treści na dowolne numery telefonów komórkowych (do pięciu numerów telefonów), dzięki czemu istotne informacje o zdarzeniach w monitorowanych obiektach mogą być wysyłane bezpośrednio do ich właścicieli i innych zainteresowanych osób. Nadajniki mają również możliwość wysyłania jawnych informacji o testach urządzenia w postaci SMS na wskazany numer, a więc końcowi użytkownicy urządzeń mogą na bieżąco kontrolować, czy instalacja chroniąca ich nieruchomość lub inny obiekt jest sprawna.

Elastyczność

Cechą nadajników PX200N jest duża elastyczność aplikacyjna – urządzenia obsługują wiele różnych typów modemów (SIMCOM SIM300C/SIM340C, Cinterion MC55, MC55i, MC56, Wavecom Q55), dzięki czemu można je dostosować do

różnych wymagań odbiorców pod względem jakości i kosztu systemu. Nadajniki mogą być również łatwo zastosowane w już istniejącym systemie alarmowym, gdyż obsługują dwa numery telefonów stacji monitorowania. Znaczną elastyczność nadajników PX200N uzyskano dzięki wyposażeniu ich w porty szeregowe – RS232 ze sprzętową kontrolą przepływu i RS485. Dzięki temu do nadajników można przyłączyć zewnętrzne urządzenia przemysłowe, zwiększając w ten sposób zakres ich stosowania.

Oszczędność

Inżynierowie, którzy zaprojektowali PX200N, mieli na uwadze także potrzebę ciągłego kontrolowania i ograniczania kosztów funkcjonowania systemów transmisji alarmów. Możliwość zdalnego konfigurowania i aktualizacji oprogramowania systemowego nie stanowi jedynie udogodnienia dla instalatorów; jest także narzędziem pozwalającym na istotne ograniczenie kosztów uruchomienia i funkcjonowania systemu. PX200N umożliwia ustalenie limitu komunikatów SMS wysyłanych przez nadajnik, co pozwala kontrolować ponoszone koszty. Wyposażono go również w funkcję przesyłania dalej przychodzących wiadomości SMS zapisywanych na zamontowanej w nim karcie SIM. Dzięki temu wiadomość od operatora sieci komórkowej o przekroczeniu limitu trafia bezpośrednio do zainteresowanych osób, które mogą na bieżąco nadzorować koszty generowane przez nadajnik.

Nadajniki PX200N zostały wyposażone w nowatorską funkcję automatycznej blokady wejść, która zabezpiecza przed generowaniem zbędnych kosztów w przypadku wystąpienia awarii (np. awarii jednej z czujek podłączonych do nadajnika). W nadajnikach, które nie mają takiego zabezpieczenia, wyeliminowanie tego problemu (czyli wysyłania fałszywych sygnałów alarmowych spowodowanych awarią) jest możliwe tylko przez całkowite wyłączenie nadajnika, czyli zmniejszenie bezpieczeństwa monitorowanego obiektu. Funkcja automatycznej blokady wejść umożliwia ustawienie parametrów, które określają, jak dużą liczbę alarmów w zadanym przedziale czasowym należy uznać za alarmy fałszywe. Wejście generujące fałszywe alarmy jest automatycznie blokowane. Możliwe jest również zaprogramowanie czasu, po jakim wejście powinno zostać odblokowane w celu sprawdzenia, czy awaria ustąpiła. Funkcja ta nie tylko pozwala wyeliminować zbędne koszty – jest również korzystna dla pracowników stacji monitoringu, którzy mają obowiązek reagowania na wszystkie alarmy. Jeśli do stacji monitorowania dochodzą sygnały fałszywych alarmów, pracownicy tracą czas, reagując na nie, a ponadto w systemie zapisują się nieprawidłowe dane, które zniekształcają historię zdarzeń i niepotrzebnie powiększają rozmiar bazy zdarzeń.

Bezpieczeństwo i niezawodność

Odpowiednie zabezpieczenie przesyłanych danych i wysoka niezawodność transmisji z nadajników to podstawowe cechy wymagane od urządzeń wspomagających ochronę osób i mienia. Nadajniki PX200N wyposażono w szereg funkcji służących do ochrony danych, zabezpieczania transmisji i eliminacji wszelkich zakłóceń. Wysoki poziom zabezpieczenia danych osiągnięto dzięki szyfrowaniu danych przesyłanych przez GPRS/SMS szyfrem AES. Przed nieautoryzowanym dostępem do nadajników chroni hasło i rozpoznawanie numeru, z jakiego przychodzą polecenia do nadajnika (nadajnik nie reaguje na komendy wysyłane z nieznanych numerów). Nadajniki wyposażono także w funkcję kontroli łącza GSM/GPRS, co zwiększa niezawodność ich działania, szczególnie w takich sytuacjach, jak zmiana firmware'u w stacjach bazowych GSM, usterki po stronie operatorów GSM czy kłopoty z połączeniem z serwerem. Nadajniki monitorują podniesienie słuchawki i bezczynność na linii telefonicznej, co pozwala przełączyć je na inny tor transmisji w przypadku awarii lini telefonicznej. Mogą obsługiwać dwa różne serwery. Jeśli nie uda im się połączyć z pierwszym serwerem, próbują transmitować dane do drugiego. Zastosowano również funkcję generacji sygnału zgłoszeniowego centrali o konfigurowalnej częstotliwości oraz symulacji linii telefonicznej o napięciu 28 V, co ułatwia komunikację z centralą alarmową. Z kolei funkcja wysokoimpedancyjnego monitorowania linii telefonicznej pozwala wyeliminować zakłócenia na linii telefonicznej, które mogą utrudniać działanie podłączonych do niej innych urządzeń (np. faksów). Warto też przypomnieć wymienianą już funkcję historii zdarzeń systemowych, która umożliwia odczytanie zapisanych w pamięci zdarzeń nawet w przypadku zniszczenia nadajnika. PX200N wyposażono także w nowatorską funkcję „usypiania" modemu, która pozwala tak zaprogramować urządzenie, aby przy niskim stanie akumulatora modem został wprowadzony w stan uśpienia. Dzięki temu można uniknąć sytuacji, w której nadajnik stara się wysyłać informację, ale nie jest w stanie dokończyć przesyłu z powodu nadmiernego rozładowania akumulatora. W ten sposób unikamy przesyłania niepotrzebnych komunikatów, dezorganizacji pracy stacji monitorowania oraz chronimy akumulator nadajnika przed całkowitym rozładowaniem skracającym jego żywotność.

Fot. 2. OSM.2007

Współpracujący z nadajnikiem PX200N Odbiornik Systemu Monitoringu OSM.2007 stanowi interfejs pomiędzy urządzeniami transmisji danych zainstalowanymi w dozorowanych obiektach a oprogramowaniem stacji monitorowania. Włączenie tego elementu w system monitorowania pozwala na tworzenie rozległych systemów telemetrycznych. Odbiorniki OSM.2007 zostały wyposażone także w szereg funkcji mających na celu podniesienie zarówno komfortu użytkowania, jak i bezpieczeństwa, niezawodności oraz elastyczności systemu.

Korzyści wynikające z zastosowania odbiornika OSM.2007

Wygoda

Odbiorniki OSM.2007 oferują łatwe zarządzanie systemem dzięki intuicyjnemu oprogramowaniu z graficznym interfejsem. Odbiornik umożliwia segregowanie i filtrowanie sygnałów według kryteriów (numerów seryjnych albo rodzaju sygnału) oraz przekazywanie danych o sygnałach bezpośrednio do bazy danych PostgresSQL. Istotną zaletą jest także to, że dzięki zastosowaniu nowoczesnych rozwiązań informatycznych osiągnięto znaczne uproszczenie procedur programowania urządzenia. W związku z tym dostosowanie trybu jego pracy do konkretnych wymagań użytkownika jest niezwykle proste. Dostęp do statystyk odbieranych sygnałów oraz konfiguracji sieciowej odbiornika jest możliwy także przez stronę WWW. Ponadto odbiorniki wyposażono w funkcję SNMP (*Simple Network Management Protocol* – Prosty Protokół Zarządzania Siecią), która jest udogodnieniem dla administratora systemu. Komfort użytkowania zwiększają funkcje automatycznej synchronizacji zegarów w urządzeniach nadawczych oraz synchronizacja czasu odbiornika z serwerem czasu NTP.

Elastyczność

Odbiorniki OSM.2007 umożliwiają przekazywanie danych do innych systemów poprzez porty RS232 (trzy porty do wyboru), konwertery USB–RS232 (trzy porty), LAN przy użyciu protokołu MLR-2 (format SIA, ContactID) lub XML. Odbiorniki obsługują urządzenia MOXA, a także wiele typów modemów GSM i wiele portów TCP/IP lub UDP. Wyposażono je również w łącza SMSC umożliwiające odbieranie komunikatów SMS bezpośrednio od operatora.

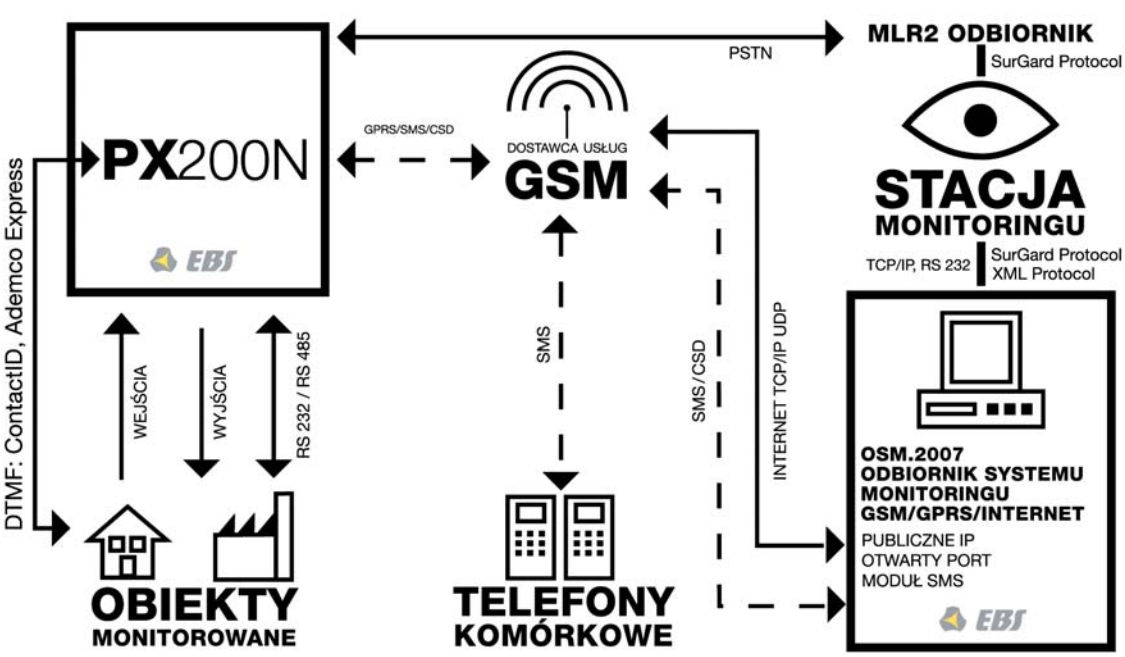
Bezpieczeństwo i niezawodność

Tak jak w przypadku nadajników, najistotniejsze są jednak funkcje poprawiające bezpieczeństwo i niezawodność urządzeń. Odbiorniki OSM.2007 wyposażono m.in. w funkcję automatycznego tworzenia kopii bezpieczeństwa całej konfiguracji nadajnika, a także szyfrowane połączenie z systemem. Urządzenia mają też funkcję automatycznego restartu systemu w przypadku jego zawieszenia się (watchdog sprzętowy), a także firewall (listy dostępu IP, limit połączeń itp.) zabezpieczający przed sabotażem i uniemożliwiający „spamowanie" serwera. Sprzęt nie posiada mechanicznego dysku twardego, a wszystkie dane zapisywane są w mniej zawodnych pamięciach typu flash. Odbiorniki OSM.2007 zapewniają większą wydajność pracy niż poprzednie wersje, dzięki czemu mogą obsługiwać do 30 000 urządzeń i do 240 000 zdarzeń na minutę.

Najważniejsze z punktu widzenia bezpieczeństwa i niezawodności całego systemu transmisji danych jest jednak zastosowanie rozwiązań redundantnych, zabezpieczających system odbiorczy na wypadek uszkodzenia jego części. Dzięki unikatowej funkcji pracy w klastrze (w grupie komputerów dublujących nawzajem swoje funkcje) w razie awarii jednej z maszyn następuje automatyczne przejęcie jej funkcji przez inny węzeł grupy. Funkcja ta zapewnia ciągłość pracy odbiornika OSM.2007 bez stałej kontroli i udziału administratora systemu.

Wszyscy użytkownicy opisanych urządzeń mogą uzyskać fachowe wsparcie techniczne – nie tylko w języku polskim, ale także angielskim, rosyjskim i hiszpańskim. Serdecznie zapraszamy do współpracy.

EBS



Rys. 1. Schemat PX200N

TargiKielce
EXHIBITION & CONGRESS CENTRE

! ALARM

X Konferencja i Wystawa Monitoringu Wizyjnego

4-5.11.2010, Kielce

Targom towarzyszą:

›› X MIĘDZYNARODOWA KONFERENCJA
„Bezpieczny Stadion"

PZPN

›› XI OGÓLNOPOLSKA KONFERENCJA
Bezpieczne Miasto - Monitoring Wizyjny Miast

Patronat prasowy: Twierdza | sa systemy alarmowe CZASOPISMO BRANŻY SECURITY | Zabezpieczenia | w akcji

Patronat internetowy: Zabezpieczenia | alarmy.com.pl GRUPA MARKETEO.COM

Targi Kielce S.A., ul. Zakładowa 1, 25-672 Kielce,
Szczegółowe informacje: Dyrektor Projektu - Grzegorz Figarski,
tel. 041 365 12 33, fax 041 345 62 61,
e-mail: figarski.g@targikielce.pl

›› **„EURO 2012 POLSKA**
- organizacja i bezpieczeństwo"

Zmiany w normie obronnej NO-04-A004

Obiekty wojskowe. Systemy alarmowe

Piotr Januszkiewicz

Norma obronna NO-04-A004 *Obiekty wojskowe. Systemy alarmowe* jest podstawowym dokumentem technicznym poświęconym wymaganiom, jakie muszą być spełnione przez stosowane w obiektach wojskowych systemy alarmowe. Norma ta w wersji z 2006 r. w części definicji i przywołań opierała się na PN-93/E-08390/14. Rozwój elektroniki, a szczególnie mikroelektroniki i optoelektroniki, spowodował gwałtowny rozwój zarówno czujek wykrywających obecność ludzi, zwierząt i ruchomych przedmiotów w strefie chronionej, jak również central alarmowych i całych systemów. Ten rozwój spowodował konieczność nowelizacji normy i dostosowania jej wymagań do współczesnego stanu technologii wykorzystywanej przez systemy alarmowe

Najważniejsze zmiany w normie obronnej NO-04-AO004 zostaną przedstawione poniżej.

Arkusz 1 – *Wymagania ogólne*

Wprowadzono definicje:

– antymaskingu,
– centrali alarmowej,
– czujki alarmowej,
– klawiatury,
– linii dozorowej,
– stanu alarmowego,
– strefy detekcji,
– stanu dozoru,
– naziemnych urządzeń alarmowych,
– ogrodzeniowych urządzeń alarmowych,
– podziemnych urządzeń alarmowych,
– usterki.

Uszczegółowiono wymagania ochrony strefy peryferyjnej

W strefie peryferyjnej nie należy instalować urządzeń alarmowych w czasie pokoju. W strefie tej utrzymuje się pas o szerokości 25 m, wolny od wysokich zarośli, krzewów i traw, umożliwiający wgląd w teren przyległy do chronionego obiektu. Pasa tego nie utrzymuje się w przypadku, gdy strefa ochrony peryferyjnej obejmuje obszar nie będący terenem wojskowym.

Określono parametry funkcjonalne systemów alarmowych:

– w przypadku linii analogowych wywoływać alarm przy odstrojeniu parametrów linii dozorowej większym niż 20%,
– w przypadku cyfrowych linii dozorowych wywoływać alarm w przypadku przerwy, zwarcia magistrali komunikacyjnej lub braku transmisji po czasie 500 ms.

Uszczegółowiono zasady budowy systemów alarmowych:

– ochronę obszarów, rejonów, terenów, obiektów i pomieszczeń jednostek wojskowych należy zawsze rozpoczynać od budowy systemów alarmowych w strefie ochrony wewnętrznej, a następnie rozszerzać instalowane systemy, zabezpieczając strefę ochrony bezpośredniej i obwodowej;
– centrale alarmowe oraz inne urządzenia nadzorujące pracę systemu alarmowego powinny znajdować się w pomieszczeniu sił ochronnych lub służb dyżurnych (w wartowni, pomieszczeniu oficera dyżurnego lub w alarmowym centrum odbiorczym), w którym pełniona jest całodobowa służba, lub w innych wydzielonych i odpowiednio zabezpieczonych pomieszczeniach;
– każde urządzenie alarmowe (czujka alarmowa, ostrzegacz napadowy) powinno być podłączone do wejścia centrali alarmowej rozróżnianego jako jedna linia alarmowa;
– wewnętrzne czujki alarmowe powinny być rozmieszczone w taki sposób, aby polem detekcji obejmowały całą chronioną powierzchnię pomieszczeń, wykluczając powstawanie tzw. martwych pól.

Arkusz 2 – *Wymagania techniczno-użytkowe*

Wprowadzono definicje:

– klawiatury lokalnej,
– kodu przymusu,
– ostrzegacza napadowego,
– rejestru zdarzeń,
– telewizyjnych systemów nadzoru.

Wprowadzono nowe wymagania dotyczące systemów alarmowych

Systemy nadzoru wizyjnego powinny być wykorzystywane przede wszystkim do weryfikacji zdarzeń alarmowych pochodzących z innych urządzeń alarmowych lub stanowić kolejny system detekcji zagrożeń wykorzystujący nowe technologie, takie jak wideodetekcja, rozpoznawanie twarzy, rozpoznawanie numerów rejestracyjnych samochodów itp.

Zrezygnowano z zapisu dotyczącego zdublowania torów transmisji alarmu z każdego podsystemu (podcentrali) do alarmowego centrum odbiorczego.

Arkusz 3 – *Metody określania liczby urządzeń*

Wprowadzono definicje:

– czujki magnetycznej,
– czujki mikrofalowej,
– czujki ultradźwiękowej,
– pionowej czujki kurtynowej,
– czujki przestrzennej,
– czujki zbicia szkła,
– pasywnej czujki podczerwieni.

Do pozostałych elementów systemu alarmowego w magazynach uzbrojenia dodano ostrzegacze napadowe.

W naliczeniach pozostałych elementów systemu alarmowego określono wymagania dotyczące schronohangarów.

Arkusz 4 – *Wymagania dotyczące urządzeń*

Wprowadzono definicje:

– sektora ochrony,
– wizyjnej detekcji ruchu,
– zewnętrznego urządzenia alarmowego.

Doprecyzowano określenie parametrów funkcjonalnych urządzeń alarmowych

Minimalny zasięg pracy czujek w bardzo złych (granicznych) warunkach atmosferycznych nie może być mniejszy niż 60% zasięgu transmisji w warunkach normalnych w przypadku urządzeń pracujących w paśmie podczerwieni oraz 80% w przypadku urządzeń mikrofalowych.

Dokonano nowego podziału urządzeń alarmowych poprzez rozróżnienie następujących rodzajów urządzeń:

1. Urządzenia ogrodzeniowe:
   – mechaniczno-odkształceniowe,
   – naprężeniowe,
   – wibracyjne i sejsmiczne
   – mikrofonowe (akustyczne),
   – światłowodowe,
   – elektrostatyczne (pojemnościowe).

2. Urządzenia naziemne:
   – bariery podczerwieni,
   – pasywne czujki podczerwieni,
   – bariery mikrofalowe,
   – czujki mikrofalowe,
   – wizyjna detekcja ruchu z wyłączeniem kamer termowizyjnych,
   – wizyjna detekcja ruchu z kamerami termowizyjnymi,
   – skanery laserowe,
   – radary.

3. Urządzenia podziemne:
   – elektromagnetyczne,
   – akustyczne,
   – magnetyczne,
   – naciskowe.

Arkusz 5 – *Wymagania dotyczące tablicy synoptycznej*

Uszczegółowiono postanowienia ogólne:

– tablica synoptyczna powinna być zaprojektowana i wykonana tak, żeby w sposób czytelny dla służb nadzorujących pracę systemu odzwierciedlała poszczególne stany systemu alarmowego rejestrowane przez centralę alarmową;
– zastosowane elementy elektroniczne powinny być energooszczędne oraz o dużej niezawodności; konstrukcja tablicy synoptycznej powinna umożliwiać jej rozbudowę w przypadku modernizacji systemu oraz zapewniać łatwy dostęp do poszczególnych jej elementów w przypadku konieczności ich naprawy lub wymiany;
– tablica powinna być urządzeniem pasywnym, pozbawionym możliwości ingerencji w pracę systemu alarmowego;
– monitor komputera może być wykorzystany jako tablica synoptyczna.

Określono wymiary tablicy synoptycznej

– minimalnym, podstawowym formatem tablicy synoptycznej powinien być format B1 (707 mm x 1000 mm). Dopuszcza się tablice o większych rozmiarach w zależności od stopnia złożoności systemu alarmowego, wielkości terenu podlegającego ochronie oraz liczby magazynów i pomieszczeń objętych ochroną;
– w przypadku tablicy synoptycznej na ekranie monitora komputerowego rozmiar monitora nie powinien być mniejszy niż 22 cale, a rozdzielczość nie mniejsza niż 1280×720 pikseli.

Arkusz 6 – *Wymagania dotyczące systemów kontroli dostępu*

Wprowadzono definicje:

– błędnej akceptacji,
– błędnego odrzucenia,
– śluzy osobowej,
– zwory elektromagnetycznej.

Do wymagań funkcjonalnych dla systemu kontroli dostępu dołączono zakaz powtórnego wejścia do obszaru, terenu, rejonu, obiektu lub pomieszczenia bez uprzedniego odnotowania wyjścia (*antipassback*).

Dodano wymóg dotyczący mechanicznych urządzeń blokujących, a mianowicie nakaz stosowania ruchomych barier zaporowych na przejściach w ogrodzeniach obiektów.

Zmieniono zapis dotyczący zasilania awaryjnego systemu kontroli dostępu

Należy mieć zasilanie integralne, niewykorzystywane do zasilania innych urządzeń, i zasilanie ze źródła rezerwowego, które zapewni normalną pracę systemu w czasie nie krótszym niż:

– 12 godzin w przypadku obiektów, w których pełnią ciągły dyżur służby serwisowe dysponujące częściami zamiennymi i zastępczymi źródłami zasilania (np. agregatami prądotwórczymi, dodatkowymi akumulatorami);
– 36 godzin w przypadku obiektów, w których istnieje ciągły dozór personelu i dla których zagwarantowane są usługi serwisowe świadczone w ciągu czterech godzin,
– 72 godziny w przypadku pozostałych obiektów, m.in. obiektów bez ciągłego dozoru personelu.

Należy zapewnić samoczynne przełączanie się zasilania ze źródła podstawowego na rezerwowe i odwrotnie, bez zakłócenia pracy systemu, a także sygnalizować w lokalnym centrum nadzoru awarie zasilania podstawowego i powrót do niego.

Arkusz 7 – *Wymagania dotyczące telewizji dozorowej*

Zmieniono tytuł arkusza na: *Obiekty wojskowe. Systemy alarmowe. Część 7. Wymagania dotyczące telewizyjnych systemów nadzoru*

Wprowadzono definicje:

– głowicy obrotowo-uchylnej,
– macierzy dyskowej,
– matrycy wizyjnej.

Uszczegółowiono wymagania ogólne

Wizyjne systemy nadzoru obejmują głównie kamery wizyjne, tory transmisyjne sygnału wizyjnego, monitory oraz rejestratory. Służą one do obserwacji wybranych stref chronionego obszaru, rejonu, terenu, obiektu oraz pomieszczenia, a także do rejestracji zdarzeń. W takich systemach należy wykorzystywać multipleksery i (lub) urządzenia rejestrujące. W strefie ochrony zewnętrznej (obwodowej i bezpośredniej) należy integrować systemy nadzoru wizyjnego z systemami alarmowymi w celu natychmiastowej weryfikacji generowanych sygnałów alarmowych przez urządzenia alarmowe zainstalowane w tej strefie. Powyższa weryfikacja powinna polegać na wyświetleniu obrazu z miejsca zdarzenia na monitorze alarmowym z jednoczesnym rozpoczęciem rejestracji zdarzenia z tzw. prealarmem. System powinien być skonfigurowany w taki sposób, aby odtworzył obraz obszaru, w którym wystąpił alarm, obejmując okres pięciu sekund przed powstaniem alarmu. Systemy nadzoru wizyjnego należy wykorzystywać także do obserwacji chronionych obszarów, rejonów, terenów, obiektów oraz pomieszczeń, stosując w nich głowice uchylno-obrotowe i obiektywy sterowane przez obsługę alarmowego centrum odbiorczego. W tym celu należy stosować pulpity sterujące. Systemy nadzoru wizyjnego mogą wykorzystywać wizyjną detekcję ruchu, której głównym zadaniem jest wykrywanie, sygnalizowanie i śledzenie określonych zmian w zdefiniowanych strefach chronionych, które znajdują się w polu widzenia kamer. Systemy nadzoru wizyjnego wyposażone w wizyjną detekcję ruchu są urządzeniami alarmowymi. Urządzenia rejestrujące obrazy z systemu nadzoru wizyjnego powinny umożliwiać odtwarzanie zdarzeń, które zaszły w systemie, z co najmniej trzech ostatnich miesięcy.

W systemach nadzoru wizyjnego, które wykorzystują kamery wizyjne z transmisją cyfrową, można stosować kamery z transmisją analogową, korzystając z konwerterów przetwarzających sygnał analogowy na cyfrowy. Rozdzielczość konwertera nie powinna być niższa niż 720×576 pikseli.

W rejonach o zwiększonym natężeniu wyładowań atmosferycznych urządzenia systemów nadzoru wizyjnego, montowane w strefach ochrony zewnętrznej, powinny być wyposażone w ochronę przeciwprzepięciową montowaną na kablach sygnałowych i zasilających. Urządzenia ochrony przeciwprzepięciowej należy umieszczać na początku i końcu linii kablowej. Stosowane urządzenia ochrony przeciwprzepięciowej powinny być klasy A.

Wyszczególniono następujące rodzaje kamer:

– kamery monochromatyczne,
– kamery kolorowe,
– kamery dualne (dzień/noc),
– kamery trójwidmowe,
– kamery termowizyjne.

Określono wymagania dla kamer termowizyjnych

Kamery termowizyjne powinny mieć rozdzielczość przetwornika nie mniejszą niż 320×240 pikseli.

W przypadku kamer telewizyjnych, w których sygnał wyjściowy jest transmitowany w postaci cyfrowej, rozdzielczość nie powinna być mniejsza niż 720×576 pikseli.

Określono wymagania dla przełączników wizji, dzielników obrazu, rejestratorów cyfrowych, matryc wizyjnych, macierzy dyskowych oraz monitorów cyfrowych, których rozdzielczość nie powinna być mniejsza niż 1280×720 pikseli.

Zmieniono zapis dotyczący zasilania awaryjnego telewizyjnego systemu nadzoru

Należy mieć zasilanie integralne, niewykorzystywane do zasilania innych urządzeń, i zasilanie ze źródła rezerwowego, które zapewni normalną pracę systemu w czasie nie krótszym niż:

– 12 godzin w przypadku obiektów, w których pełnią ciągły dyżur służby serwisowe dysponujące częściami zamiennymi i zastępczymi źródłami zasilania (np. agregatami prądotwórczymi, dodatkowymi akumulatorami);
– 36 godzin w przypadku obiektów, w których istnieje ciągły dozór personelu i dla których zagwarantowane są usługi serwisowe świadczone w ciągu czterech godzin;
– 72 godziny w przypadku pozostałych obiektów, m.in. obiektów bez ciągłego dozoru personelu.

Należy zapewnić samoczynne przełączanie się zasilania ze źródła podstawowego na rezerwowe i odwrotnie, bez zakłócenia pracy systemu, a także sygnalizować w lokalnym centrum nadzoru awarie zasilania podstawowego i powrót do niego.

Opracowano nowy arkusz – *Obiekty wojskowe. Systemy alarmowe. Część 9. Wymagania dotyczące monitorowania alarmów*

W tym arkuszu normy podano wymagania techniczno-użytkowe dla oddalonych centrów monitorowania alarmów oraz dla obiektów wojskowych, które będą przez te centra monitorowane. Określono również wymagania dla podmiotów gospodarczych zajmujących się monitorowaniem systemów zabezpieczeń w obiektach wojskowych.

mgr inż. Piotr Januszkiewicz

Wirtualizacja

Klastry wysokiej dostępności

Paweł Duda

Od obecnej infrastruktury serwerowej wymaga się ciągłego i nieprzerwanego działania. Serwery – np. plikowe, WWW, bazodanowe itp. – muszą być dostępne dla użytkowników nieprzerwanie, przez całą dobę i siedem dni w tygodniu. Dla wielu firm, a w zasadzie dla ich działów IT, jest to podstawowa zasada funkcjonowania systemów komputerowych. Z pomocą przychodzi klastrowanie serwerów lub usług. Klaster serwerów to grupa serwerów widocznych dla użytkowników jako jeden system (jako jeden serwer lub jako jedna aplikacja) zapewniający wysoką dostępność (HA – *High Availability*) do krytycznych aplikacji i danych. Klastry mogą być wykorzystywane m.in. do utrzymywania bardzo obciążonych usług sieciowych (np. serwerów WWW). Takie klastry nazywane są klastrami równoważącymi obciążenie (*Load Balancing Cluster*) lub klastrami serwerowymi

Oczywiście klastrowanie to nie tylko powielanie serwerów, ale również redundancja połączeń tych serwerów z sieciami komputerowymi, zasilania, połączenia z zasobami dyskowymi (macierzami), pełna redundancja elementów samej macierzy (kontrolerów, zasilaczy, połączeń z serwerami).

Zazwyczaj dobór klastrów o wysokiej dostępności jest trudny i wiąże się z wysokimi kosztami. Wirtualizacja umożliwia tworzenie klastrów HA bez ponoszenia dodatkowych kosztów związanych z zastosowaniem fizycznych rozwiązań klastrowych. Warunkiem jest posiadanie serwerów wirtualizacyjnych i odpowiednich licencji.

Na wirtualnej platformie można uzyskać klastry o wysokiej dostępności na dwóch poziomach. Pierwszy poziom ogranicza się do monitorowania hosta (serwera fizycznego), drugi zaś synchronizuje maszyny wirtualne będące w klastrze i stany połączeń z tymi maszynami.

Co to jest – fizycznie – klaster HA serwerów wirtualnych? Jest to zespół serwerów działających na rzecz wspólnego dobra, jakim jest ciągłe działanie wirtualnych maszyn uruchomionych na wszystkich hostach należących do klastra HA. Wyznaczone serwery w klastrze HA posiadają wszystkie informacje o uruchomionych maszynach wirtualnych – na którym hoście dana maszyna jest uruchomiona, jakie ma przydzielone zasoby i priorytety, jaka jest ścieżka do katalogu z plikami konfiguracyjnymi danej maszyny itp.

Podczas konfiguracji klastra HA administrator definiuje liczbę fizycznych serwerów (hostów) w klastrze, które mogą ulec awarii. W zależności od tej wartości klaster HA oblicza, ile wirtualnych maszyn może zostać uruchomionych jednocześnie w całym klastrze. Informacja ta jest wymagana, aby w danym klastrze HA nie uruchomić zbyt dużo maszyn. Administrator może wyłączyć funkcję informowania i zapobiegania uruchomieniu zbyt dużej liczby wirtualnych maszyn, co jednak nie jest zalecane. Jak widać, klaster taki rezerwuje zasoby na potrzeby HA w zależności od liczby zdefiniowanych hostów, które mogą ulec awarii. Jeśli w klastrze mamy trzy identyczne serwery i zdefiniujemy, że awarii może ulec jeden, to HA pozwoli nam uruchomić tyle wirtualnych maszyn, ile będzie zasobów na dwóch serwerach. System działa w ten sposób, ponieważ w momencie awarii jednego hosta z trzech zostają tylko dwa, na których muszą uruchomić się wszystkie wirtualne maszyny z hosta, który uległ awarii. Jeśli w klastrze HA mamy niesymetryczne serwery (serwery nie są identyczne, np. jeden posiada więcej pamięci operacyjnej), to algorytm z całych zasobów klastra, na poczet awarii, odlicza zasoby najmocniejszych serwerów hostów.

Jak wynika z powyższego opisu, taki klaster HA nie jest klastrem idealnym. Można go zastosować dla serwerów wirtualnych, w przypadku których biznesowo mamy zezwolenie na niedostępność rzędu 5–10 minut, w zależności od zastosowanego sprzętu oraz oprogramowania wirtualizacyjnego. Wynika to z tego, iż w momencie awarii danego hosta fizycznego

klaster zauważy jego brak i uruchomi brakujące maszyny wirtualne na pozostałych zasobach klastra. Proszę zwrócić uwagę na to, że klaster uruchomi brakujące maszyny od zera, tzn. wirtualne serwery nie będą dostępne w czasie ich uruchamiania. Ponadto wszystkie nawiązane sesje do tych serwerów zostaną utracone. Jest to logiczne, gdyż uszkodzeniu uległ host, na którym te maszyny pracowały, a klaster uruchamia je od nowa na pozostałych zasobach.

Jak już wspomniałem, taki rodzaj klastra nadaje się do systemów, które mogą być niedostępne przez kilka minut. Mogą to być np. kontrolery domen, serwery WWW, ftp, pamięć podręczna serwerów pocztowych, same serwery pocztowe itp. Zalety takiego klastrowania to niska cena (licencja tylko na wirtualizację, a klastrować można wszystkie maszyny wirtualne) oraz łatwość implementacji i obsługi. Nie są potrzebne dodatkowe licencje na system operacyjny i aplikacje pracujące w wirtualnej maszynie. Wady: utrata połączeń z wirtualnymi maszynami w momencie awarii i ich niedostępność w czasie uruchamiania.

Drugi rodzaj klastra zapewnia nieprzerwany dostęp do wirtualnej maszyny. Jego działanie opiera się na monitorowaniu hostów (jak w poprzednim przypadku) oraz – dodatkowo – na powieleniu wirtualnej maszyny. Maszyna wirtualna pracuje na pierwszym hoście, natomiast na drugim system wirtualizacji tworzy kopię tej maszyny i cały czas na bieżąco synchronizuje stan tej maszyny ze stanem oryginału. Takie rozwiązanie zapewnia ciągły dostęp do wirtualnej maszyny, nawet w przypadku awarii hosta. Zalety takiego rozwiązania to względnie niska cena i łatwość implementacji. Ten rodzaj klastrowania daje wysoką dostępność, ale należy pamiętać, iż jedna maszyna wirtualna jest uruchomiona dwa razy (na dwóch hostach), a w związku z tym wymagane są podwójne zasoby dla tej maszyny wirtualnej oraz podwójne licencje na system operacyjny oraz aplikacje, które są zainstalowane w maszynie wirtualnej. Do wykonania klastra na maszynach fizycznych również wymagane są licencje i dodatkowe zasoby w postaci fizycznego serwera.

Oczywiście oba rodzaje klastrów mogą pracować równocześnie, czyli klaster HA działa we wszystkich maszynach wirtualnych, a w wybranych wykonujemy dodatkowo klaster drugiego rodzaju i uruchamiamy kopię maszyny wirtualnej.

Jak widać, klaster maszyny wirtualnej jest prosty w implementacji i niezbyt kosztowny. Aby dobrać odpowiedni rodzaj klastra do poszczególnych serwerów wirtualnych, przed wdrożeniem należy zawsze wykonać projekt ze szczególnym uwzględnieniem dopuszczalnych czasów niedostępności maszyn, które mają być klastrowane.

Podsumowując, można powiedzieć, iż zaletą wirtualizacji jest zapewnienie wysokiej dostępności przy jednoczesnym zachowaniu niskich kosztów.

Paweł Duda
OPTeam

Pronto – Drukarka do kart identyfikacyjnych

Pronto

MAGICARD

Mała, kompaktowa drukarka o nowoczesnym wyglądzie do zastosowania w każdej firmie i w każdym miejscu. Do szybkiego drukowania identyfikatorów oraz różnego rodzaju kart plastikowych. Drukarka Pronto jest łatwa w konfiguracji i użytkowaniu, posiada instrukcję i sterowniki w języku polskim do Windows 2000, XP, Vista, 7 i zapewnia niezawodne drukowanie kart przez wiele lat. Drukarka Magicard Pronto umożliwia wykorzystanie HoloKote™ i HoloPatch™ – opatentowanych zabezpieczeń przed nieautoryzowanym kopiowaniem kart.

Dzięki drukarce Pronto samodzielnie wykonasz kolorowe i monochromatyczne nadruki wysokiej jakości.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund
- Monochromatyczny wydruk karty w 7 sekund
- TRW - Thermal Rewritable (wielokrotny zadruk termiczny)
- Interfejs do PC: USB rev. 1.1. (kompatybilny z USB 2.0)
- Sterowniki w języku polskim: Windows 2000, XP, Vista, 7
- Rozdzielczość wydruku: 300 dpi
- Zasilanie: 90-265 V / 47-63 Hz
- Wymiary / Masa: 270 mm × 215 mm × 233 mm / 4,4 kg
- Temperatura pracy: od 10°C do 30°C
- Gwarancja: 2 lata

Taśmy

- YMCKO 5 paneli nadruk 300 kart (MA300YMCKO)
- YMCKO 5 paneli nadruk 100 kart (MA100YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna zielona nadruk 1000 kart (MA1000K-GREEN)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR-80 (85,6 × 54) oraz CR-79 (84,1 × 52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch i kartach do wielokrotnego zadruku TRW.

Zestaw czyszczący

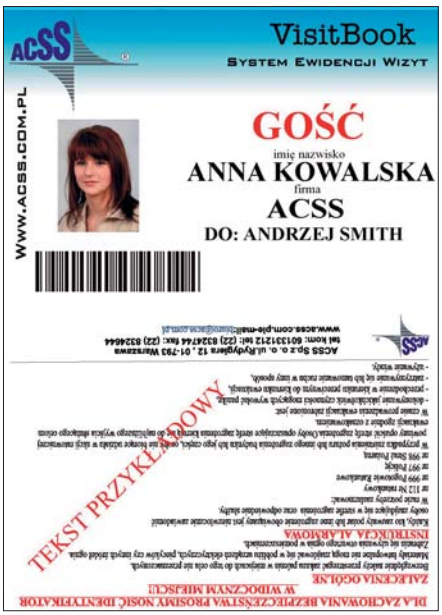
- 1 szt. rolki czyszczącej dostarczanej z każdą taśmą
- 10 szt. kart czyszczących, 1 flamaster (CK1)
- 5 wałków czyszczących plus wymienna oś wałka

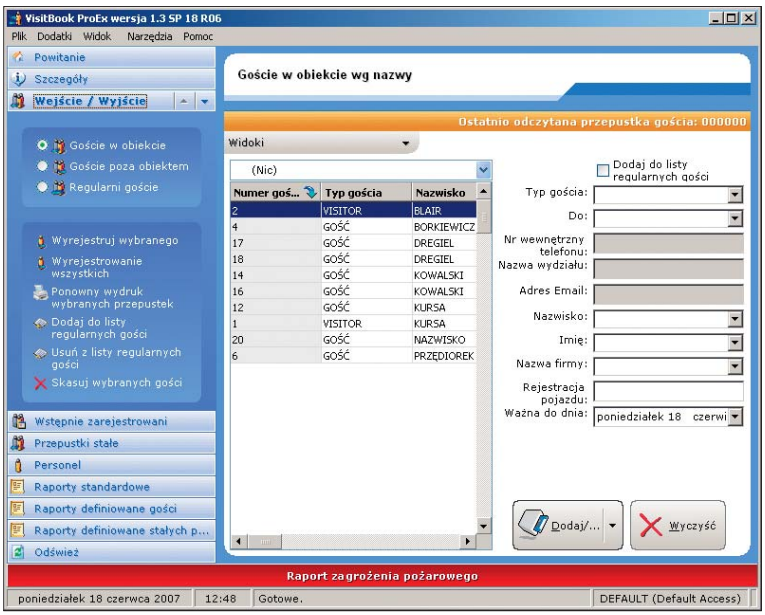
Dystrybucja:

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

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: menedżer personelu, menedżer kontrahentów, obsługa konferencji.

Dystrybucja:

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

GOLD-PLUS inteligentny tester akumulatorów z ręczną kalibracją

Inteligentny Tester Akumulatorów GOLD-PLUS został zaprojektowany do testowania akumulatorów 6-voltowych o pojemności od 1,2 h do 12 Ah oraz 12-voltowych o pojemności od 1,2 Ah do 100 Ah. Zastosowana technologia symulacji pełnego rozładowania skraca normalny test rozładowania z 20 godzin do 20 sekund. Automatycznie wyświetla napięcie akumulatora i aktualną pojemność. Dzięki funkcji kalibracji testera możliwe jest testowanie szczelnych akumulatorów (SLA) wykonanych w technologii AGM, żelowych do pracy cyklicznej oraz akumulatorów samochodowych. Akumulatory można testować wielokrotnie bez przerw pomiędzy pomiarami. Wbudowana dioda LED ostrzega przed odwróceniem polaryzacji.

Wymiana akumulatora jest zalecana, jeżeli jego współczynnik pojemności spada poniżej 65%. Na obudowie umieszczona jest tabela referencyjna wskazująca, kiedy akumulator powinien zostać doładowany lub wymieniony.

Cechy charakterystyczne

- Testuje w ciągu 20 sekund 6- i 12-voltowe szczelne akumulatory (SLA) - AGM i żelowe oraz akumulatory samochodowe,
- automatycznie wyświetla napięcie akumulatora i aktualną pojemność,
- może być skalibrowany do testowania akumulatorów szczelnych, żelowych i samochodowych o pojemności od 1,2 Ah do 100 Ah,
- zabezpieczony przed odwróceniem polaryzacji,
- testuje akumulatory szybko, dokładnie i jest łatwy w użyciu,
- zastosowanie – akumulatory w systemach alarmowych, zasilaczach UPS, samochodach elektrycznych i spalinowych.

Parametry techniczne	
Model	GOLD- PLUS
Typy akumulatorów	szczelne (SLA) – AGM i żelowe samochodowe akumulatory obsługowe
Pojemność akumulatorów	6 V 1,2 Ah – 12 Ah oraz 12 V 1,2Ah – 100 Ah
Impulsowe obciążenie akumulatora podczas pomiaru	6 A dla akumulatorów 1,2Ah – 9,9Ah, 18 A dla akumulatorów 10Ah – 100Ah
Kalibracja Ah	Kalibrowany w pozycji 0 dla nowego, w pełni naładowanego akumulatora SLA o temperaturze 20-25 °C. Regulacja kalibracji w zakresie 00-99 dla akumulatorów żelowych i samochodowych
Wyświetlacz	podświetlany LCD
Ostrzeżenie o odwróconej polaryzacji	czerwona dioda LED
Ostrzeżenie o zbyt niskim napięciu akumulatora	dla 6V < 5,25 V_{DC}, dla 12 V <12,0 V_{DC}
Tolerancja pomiaru Ah	+/- 10 % (zależy od konstrukcji i parametrów produkcyjnych)
Tolerancja pomiaru VDC	+/- 2 %
Zabezpieczenie odwrócenia polaryzacji	tak
Zdolność wykonania kolejnych testów	natychmiastowa
Obudowa	ABS
Szczelność	IP54
Wymiary	210 mm × 110 mm × 41 mm
Masa	600 g (w opakowaniu)
Wyposażenie	Przewody testowe, futerał, certyfikat zgodności, etykiety na akumulatory
Gwarancja	1 rok

Dystrybucja: 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

bibi-R33

Czytnik transponderów odporny na warunki atmosferyczne

Czytnik bibi-R33 odczytuje identyfikator kart Philips Mifare®. Karty (breloczki) tego typu są powszechnie stosowane jako karty miejskie (np. bilety komunikacji miejskiej) czy legitymacje studenckie, które dodatkowo można wykorzystywać jako identyfikatory w systemach kontroli dostępu i rejestracji czasu pracy.

Czytnik bibi-R33 współpracuje z kontrolerem dostępu bibi-K12 przesyłając do niego odczytane numery identyfikacyjne kart poprzez interfejs RS232. Dodatkowo kontroler w odpowiedni sposób steruje diodami świecącymi i brzęczykiem w czytniku.

Czytnik wykonany jest w trwałej, estetycznej obudowie z ABSu w kolorze czarnym lub jasnoszarym. Wszystkie elementy elektroniczne zalane są masą wepuranową, co czyni czytnik odpornym na warunki atmosferyczne. Czytnik może być instalowany zarówno wewnątrz jak i na zewnątrz budynku.

Dane techniczne	
Zasilanie	12V DC, 60mA
Identyfikatory	Philips Mifare®
Odczyt	13,56 MHz
Zasięg odczytu	minimum 5 cm
Sygnalizatory	diody LED + brzęczyk
Połączenie z kontrolerem	interfejs RS232 9600 8N1
Długość połączenia	do 20 m
Temperatura pracy	od 30°C do +70°C
Wymiary	50×105×14 mm
Dostępne kolory	jasnoszary, czarny

Zastosowana technologia umożliwia montaż czytnika bibi-R33 bezpośrednio na metalowej powierzchni bez utraty zasięgu odczytu kart.

Odpowiednia konstrukcja czytnika pozwala na umieszczanie go bezpośrednio na powierzchni ściany, podkładania szyldów zaprojektowanych stosownie do wystroju wnętrza (w biurowcu lub hotelu) oraz na zagłębieniu czytnika bezpośrednio w ścianę gipsową, profil aluminiowy lub obudowę maszyny.

Dostępna jest wersja czytnika z interfejsem Wiegand'a, przeznaczona do pracy z kontrolerami dostępu innych producentów.

Produkcja:

Micromade Gałka i Drożdż sp.j.
ul. Wieniawskiego 16
64-920 Piła

tel./faks (67) 213 24 14
e-mail: mm@micromade.pl
http://www.micromade.pl

Kamera szybkoobrotowa (Speed Dome) S1765P

Kamera szybkoobrotowa (Speed Dome) S1765P o bardzo wysokiej czułości i rozdzielczości 480 TVL jest wyposażona w system DSS – Digital Slow Shutter pozwalający na zwiększenie czułości przy niedostatecznym poziomie oświetlenia.

Kamera cechuje się nieograniczonym 360° obrotem w poziomie oraz posiada funkcję Auto-Flip, czyli automatycznej zmiany położenia modułu przy obrocie w pionie.

Zalety:

- zwiększająca czułość funkcja DSS (Digital Slow Shutter) regulowana w zakresie do 128 obrazów,
- mechanicznie odsuwany filtr IR
- pełny obrót 360° – ciągły obrót kamery,
- zoom całkowity x270
- 8 stref prywatności
- menu ekranowe OSD
- sterowanie z rejestratorów Commax CSD-40HA, CSD-80HA oraz CSD-160HA za pomocą portu RS-485
- możliwość mocowania do słupa, ściany, sufitu oraz narożnika ściany
- szybkość obrotu w poziomie 360°/s

Właściwości:

- kamera dzień/noc
- przetwornik 1/4" Super HAD
- wysoka rozdzielczość 480 TVL
- tryb czarno/biały w trudnych warunkach oświetlenia
- czułość: 1,0 lx (tryb kolorowy), 0,5 lx (tryb b/w), 0,001 lx (tryb DSS) przy poziomie sygnału 30IRE
- 27 krotny zoom optyczny, 10 krotny zoom cyfrowy
- 127 presetów
- 8 tras automatycznego skanowania
- 4 makra, 8 grup
- OSD
- AGC, BLC, AWB, Flickerless, tryb przełączania dzień/noc
- funkcja lustrzanego odbicia (mirror)
- zasilanie 24V AC

Dane techniczne	
Model	S2965PX
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/4" SONY Super HAD CCD
Rozdzielczość efektywna	752(H) x 582(V) 440K
Liczba linii	480 TVL
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>48 dB (AGC wył.)
Obiektyw	f = 3,6~97,2 m, F1,6~3,9
Zoom	27× optyczny, 10× cyfrowy
Ostrość	auto / ręcznie / półautomatycznie
Tryb dzień/noc	mechaniczny filtr IR
Czułość	1,0 lx / 0,5 lx(b/w) / 0,001 lx (DSS x128) 30IRE
Menu OSD	jęz. angielski
Balans bieli	automatyczny / ręczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Ostrość	automatyczna / ręczna / półautom.
Kompensacja światła tylnego	BLC, Wł. / Wył., strefowa
Redukcja migotania	Wł. / Wył.
Jasność	regulowana
Strefy prywatne	8 programowalnych stref
Elektroniczna migawka	1/50~1/10 000 s
Ręczna migawka	1/50 ~ 1/10 000 s
Obrót w pionie	90° w pionie
Obrót w poziomie	360° w poziomie
Prędkość obrotu	maks. prędkość 360°/s
Zmiana prędkości obrotu	1~360°/s (proporcjonalna od zoom'u)
Dokładkość pozycjonowania	0,25°
Presety	127 z indywidualną regulacja parametrów obrazu
Skanowanie	8
Makra	4
Grupy	8
Inne	Auto Flip, Auto Parking, wznawianie ruchu po zaniku zasilania, Freeze in Preset, RS-485
Obsługiwane protokoły	Pelco-D, Pelco-P
Stopień ochrony IP	IP66
Wejścia/wyjścia alarmowe	4/2
Zasilanie	24 V_{AC} (19~29 V_{AC})
Pobór prądu	maks. 2 A / 48 VA
Wymiary (średnica × wys.)	fi 149 mm / fi 163,6 × 230,9mm (bez pierścienia maskującego)
Temperatura pracy / Wilgotność	–30°C ~ 50°C / 30% ~ 80% RH
Masa	3,5 kg / 0,768 kg uchwyt ścienny / 0,880 kg uchwyt sufitowy / 0,984 kg mocowanie podtynkowe
Zastosowanie	kamera Speed Dome zewnętrzna

Dystrybucja: &GDE POLSKA

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

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

Kamera szybkoobrotowa (Speed Dome) S2965PX

Kamera szybkoobrotowa (Speed Dome) S2965PX o bardzo wysokiej czułości i rozdzielczości 530 TVL jest wyposażona w system DSS – Digital Slow Shutter pozwalający na zwiększenie czułości przy słabym oświetleniu.

W kamerze zastosowano przetwornik Exview HAD. Kamera cechuje się nieograniczonym obrotem o 360°, funkcją Auto-Flip oraz szerokim zakresem dynamiki WDR.

Zalety:

- zwiększająca czułość funkcja DSS (Digital Slow Shutter) regulowana w zakresie do 128 obrazów,
- szeroki zakres dynamiki WDR (Wide Dynamic Range)
- mechanicznie odsuwany filtr IR, pełny obrót o 360° – kamera może obracać się w sposób ciągły
- zoom całkowity x432
- 8 stref prywatności
- menu ekranowe OSD
- sterowanie z rejestratorów Commax CSD-40HA, CSD-80HA oraz CSD-160HA za pośrednictwem portu RS-485
- możliwość mocowania do słupa, ściany, sufitu oraz narożnika ściany
- obudowa IP66
- szybkość 360°/s

Właściwości:

- kolorowa kamera dzień/noc
- przetwornik 1/4" Exview HAD
- wysoka rozdzielczość 530 TVL
- tryb czarno/biały w trudnych warunkach oświetlenia
- 1,4 lx (tryb kolorowy), 0,1 lx (tryb kolorowy, DSS), 0,01 lx (tryb B/W, DSS)
- 36 krotny zoom optyczny, 12 krotny zoom cyfrowy
- 127 presetów
- 8 tras automatycznego skanowania
- 4 makra, 8 grup
- OSD
- AGC, BLC, AWB, Flickerless, D/N – regulacja przez OSD
- funkcja odbicia lustrzanego (mirror)
- grzałka i wentylator
- zasilanie 24V AC

Dane techniczne	
Model	S2965PX
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/4" SONY ExView CCD
Rozdzielczość efektywna	752(H) × 582(V) 440K
Liczba linii	530 TVL
WDR	Wł./Wył.
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB (AGC wył.)
Obiektyw	f = 3,4~122,4 m, F1,6~4,5
Zoom	36× optyczny, 12× cyfrowy
Ostrość	auto / ręcznie / półautomatycznie
Tryb dzień/noc	mechaniczny filtr IR
Czułość	1,4 lx / 0,1 lx(kolor,DSS) / 0,01 lx (b/w DSS x128) 50IRE
Menu OSD	jęz. angielski
Balans bieli	automatyczny / ręczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Ostrość	automatyczna / ręczna-półautom.
Kompensacja światła tylnego	BLC, Wł. / Wył., strefowa
Redukcja migotania	Wł. / Wył.
Jasność	regulowana
Strefy prywatne	8 programowalnych stref
Elektroniczna migawka	1/3~1/10 000 s
Ręczna migawka	1/3 ~ 1/10 000 s
Obrót w pionie	90° w pionie
Obrót w poziomie	360° w poziomie
Prędkość obrotu	maks. prędkość 360°/s
Zmiana prędkości obrotu	1~360°/s (zależne od zoom)
Dokładkość pozycjonowania	0,25°
Presety	127 z indywidualną regulacja parametrów obrazu
Skanowanie	8
Makra	4
Grupy	8
Inne	Auto Flip, Auto Parking, wznawianie ruchu po zaniku zasilania, Freeze in Preset, RS-485
Obsługiwane protokoły	Pelco-D, Pelco-P
Stopień ochrony IP	IP66
Wejścia/wyjścia alarmowe	4/2
Zasilanie	24 V_{AC} (19~29V_{AC})
Pobór prądu	maks. 2 A / 48 VA
Wymiary (średnica × wys.)	fi 150 mm / fi 210 × 355 mm (z uchwytem) / fi 250 x 355 mm (z uchwytem i osłoną przeciwsłoneczną)
Temperatura pracy / Wilgotność	-30°C ~ 50°C / 30% ~ 80% RH
Masa	3,8 kg / 4,3 kg z osłoną przeciwsłoneczną
Zastosowanie	kamera Speed Dome zewnętrzna

Dystrybucja: &GDE POLSKA

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

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

16-kanałowy rejestrator HDS4848DV

CNB TECHNOLOGY Inc.

16-kanałowy rejestrator HDS4848DV posiada wysoko rozwinięte możliwości pracy sieciowej oraz nowoczesny algorytm kompresji H-264. Czynnikiem wyróżniającym rejestrator jest bardzo wydajny algorytm kompresji H.264 oraz oprogramowanie typu CMS (Central Monitoring System) do zdalnego zarządzania rejestratorami, o nazwie HDxViewer.

Specyfikacja

- Algorytm kompresji H.264
- 4 poziomy kompresji (Low, Normal, Fine, Best)
- Praca w trybie Pentaplex
- Prędkość zapisu 400 kl./s@CIF, 200 kl./s@HalfD1, 100 kl./s@D1
- Nagrywanie ciągłe, detekcji ruchu, alarmowe definiowane w harmonogramie
- Wejścia przelotowe
- Sterowanie za pomocą: klawiatury, pilota IR, myszy USB lub za pomocą aplikacji sieciowej HdxViewer (CMS)
- Przycisk nagrywania napadowego
- Rozbudowane możliwości przeszukiwania nagrań w tym po zdarzeniach alarmowych (np. ruch) oraz po czasie
- Sterowanie wieloma DVR z jednej klawiatury
- Pełne zarządzanie rejestratorem przez sieć
- Dwukierunkowa komunikacja głosowa między klientem sieciowym a rejestratorem
- Synchronizacja czasu z serwerem czasu NTP
- Możliwość montażu do 3 dysków SATA o pojemności do 1TB w wersji z wbudowaną nagrywarką DVD-RAM albo 4 dysków SATA bez nagrywarki
- Obsługa dynamicznych adresów IP (serwer DDNS)
- Zapis nagrań w formacie Quick Time
- Funkcja mirroringu
- 4 porty USB, w tym 3 przeznaczone do podłączenia dysków USB, 1 port USB przeznaczony dla myszy
- Współpraca z systemami POS/ATM
- Menu w języku polskim

Rejestrator pozwala na zapis do 100 kl./s w rozdzielczości D1 (720x576) w każdym z kanałów.

Detekcja ruchu, aktywacja wejść alarmowych oraz inne zdarzenia systemowe (przegrzanie dysku, zmiana stanu wejść alarmowych) może aktywować wyjście przekaźnikowe i tym samym sterować włączeniem światła, syreny alarmowej itp.

Pełna możliwość pracy w sieci oznacza że całość czynności związanych z obsługą rejestratora można dokonać zdalnie. W systemie można zdefiniować kilku użytkowników o różnych poziomach dostępu do zasobów rejestratora.

Dostępne są także rejestratory w wersji 4-kanałowej: HDF1212 (100 kl./s@CIF, 1xHDD) oraz 16-kanałowej: HDS4824 (100 kl./s@D1, 3xHDD, opcjonalny 1XODD).

Informacje dodatkowe

- Wyjście VGA oraz aż 4 dodatkowe wyjścia monitorowe (typu spot)
- Obsługa dysków twardych oraz napędów optycznych SATA
- Wygodny tryb wyszukiwania oraz odtwarzania nagrań
- Łatwa obsługa dzięki przejrzystemu i intuicyjnemu menu
- Zapis typu pre-alarm i post-alarm
- Łatwa archiwizacja danych przez złącze USB na pamięci Flash
- Obsługa kamer PTZ
- Podgląd za pomocą przeglądarki IE (dostęp do ustawień, podglądu on-line oraz odtwarzania nagrań)
- Ustawienia parametrów obrazu indywidualnie dla każdej kamery

Dystrybucja: &GDE POLSKA

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

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

Kamera kopułowa DFL-11S

CNB TECHNOLOGY Inc.

MONALISA

Kamera kopułowa DFL-11S o wysokiej czułości i rozdzielczości 420 TVL w trybie kolorowym wyróżnia się wiernym odwzorowaniem kolorów. Kolory są żywe i naturalne, a obraz ostry i wyraźny. Kamera przeznaczona jest do zastosowań wewnętrznych. W kamerze zastosowano procesor DSP Monalisa. Odpowiednikiem kamery DFL-11S o wyższej rozdzielczości 600 TVL jest model DFL-21S.

Zaletami kamery są:

- 3-osiowa regulacja położenia modułu kamerowego: pionowa, pozioma oraz obrót wokół własnej osi
- SBLC – ulepszona funkcja kompensacji tylnego oświetlenia BLC

Właściwości:

- kamera dzień/noc
- przetwornik 1/3" Sony Super HAD
- rozdzielczość 420 TVL
- czułość 0,05 lx (kolor)
- obiektyw 3,8 mm
- AGC, SBLC, AWB
- zasilanie 12 V_{DC}
- obudowa kopułowa o średnicy 85 mm

Dane techniczne	
Model	DFL-11S
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD
Rozdzielczość efektywna	752(H) × 582(V) 440K
Liczba linii	420 TVL
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB
Obiektyw	f=3,8 mm
Tryb dzień/noc	auto
Czułość	0,05 lx
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja światła tylnego	SBLC, automatyczna
Elektroniczna migawka	1/50~1/120 000 s
Zasilanie	12 V_{DC}
Pobór prądu	maks. 150 mA
Wymiary (średnica x wys.)	113,2 × 79,15 mm
Temperatura pracy / Wilgotność	-10°C~45°C / 30%~80% RH
Masa	150 g

Dystrybucja: &GDE POLSKA

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

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

Elektrozaczepy SCOT

Elektrozaczep jest elementem wykonawczym kontroli dostępu, tzn. realizuje fizyczne zwolnienie skrzydła drzwi przez system domofonowy, wideodomofonowy, kontroli dostępu lub też prosty przycisk zwierny (tzw. „dzwonkowy").

Elektrozamki SCOT wytwarzane są z wysokiej jakości materiałów, co przekłada się na ich bezawaryjną pracę przez długi okres. Testy producenta nie wykazują nadmiernego zużycia nawet przy setkach tysięcy cykli otwarcia. Pozwala to na objęcie elektrozamka 5-letnią gwarancją. Wraz z elektrozamkiem klient otrzymuje uniwersalną, metalową listwę umożliwiającą montaż elektrozamka w słupku furtki lub w ościeżnicy drzwi.

cecha / model	symetryczny	regulacja języka	napięcie zasilania	standardowy (NC)	rewersyjny (NO)	pamięć	blokada	sygnalizacja
ES-S12AC/DC	+	+	12 $V_{AC/DC}$	+				
ES-S12AC/DC-M	+	+	12 $V_{AC/DC}$	+		+		
ES-S12AC/DC-B	+	+	12 $V_{AC/DC}$	+			+	
ES-S12AC/DC-MB	+	+	12 $V_{AC/DC}$	+		+	+	
ES-S12DCn	+	+	12 V_{DC}	+				
ES-S12DC-R	+	+	12 V_{DC}		+			
ES-S12DC-RS	+	+	12 V_{DC}		+			+
ES-S24AC/DC	+	+	24 $V_{AC/DC}$	+				
ES-S24DC-R	+	+	24 V_{DC}		+			
ES-S24DC-RS	+	+	24 V_{DC}		+			+

Elektrozaczep symetryczny

W przypadku typowych modeli, klient przy wyborze elektrozamka musi określić kierunek otwierania sterowanych nim drzwi (lewy-prawy). Elektrozaczep symetryczny posiada zapadkę (język) umieszczony w jednakowej odległości od obu krawędzi obudowy, co sprawia, że można go montować zarówno w drzwiach lewych jak i prawych. Eliminuje to konieczność doboru konkretnego rodzaju elektrozamka już na etapie projektowania systemu kontroli wejścia.

Regulacja języka zapadki

Pozwala na eliminację szczeliny pomiędzy językiem (zapadką) elektrozaczepu, a zapadką zamka drzwi przez wysunięcie języka elektrozaczepu w zakresie 0 ~ 4 mm od standardowego położenia.

Blokada mechaniczna

Elektrozaczep posiada mechaniczny przełącznik, który umożliwia rezygnację z kontroli otwarcia wejścia. Ma zastosowanie w miejscach, gdzie w ciągu dnia jest duże natężenie ruchu osobowego i nie ma wymogu, aby drzwi były zabezpieczone przed wejściem.

Pamięć

Do otwarcia (odblokowania) zamka wystarczy krótki (chwilowy) impuls elektryczny, który powoduje odblokowanie elektrozaczepu. Po otwarciu skrzydła drzwi elektrozaczep powraca do stanu zamkniętego. Jest to wygodna funkcja w przypadku zastosowania przycisku wyjścia umieszczonego w pewnej odległości od drzwi, gdzie osoba wychodząca nie może jednocześnie nacisnąć przycisku wyjścia i otworzyć drzwi.

Sygnalizacja

Elektrozaczep jest wyposażony w mikroprzełącznik z zaciskami, który całkowicie zastępuje dodatkowe elektromagnesy instalowane w drzwiach. Umożliwia to dodatkowo kontrolę stanu wejścia (np. kontrolę niedomkniętych drzwi), podając sygnał do systemu kontroli lub centrali alarmowej.

Uniwersalne zasilanie

Elektrozaczep został wyposażony w cewkę pozwalającą na zasilanie prądem stałym (z zasilacza prądu stałego) lub zmiennym (z transformatora). Właściwość ta pozwala na montaż elektrozaczepów SCOT w systemach posiadających już zainstalowane źródło ich zasilania.

Elektrozaczep rewersyjny

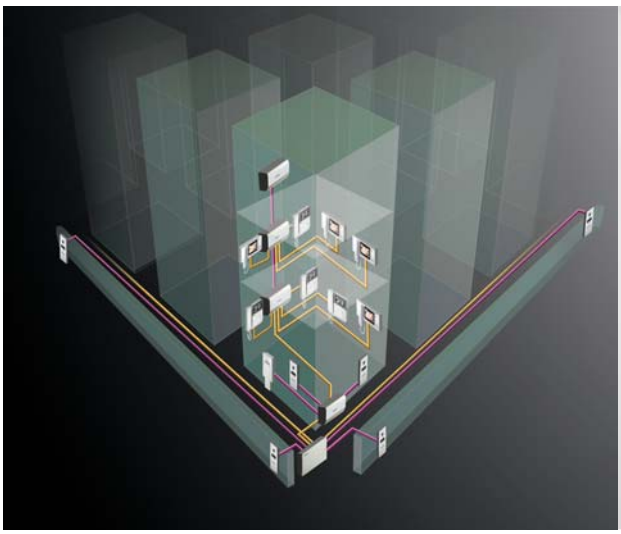
Elektrozamek z odwrotną funkcją otwarcia. Zamek rewersyjny jest po podłączeniu napięcia zasilającego zamknięty (zablokowany). Po odłączeniu zasilania zamek jest otwarty (odblokowany).

Dystrybucja: &GDE POLSKA

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

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

System wieloabonentowy serii 2400

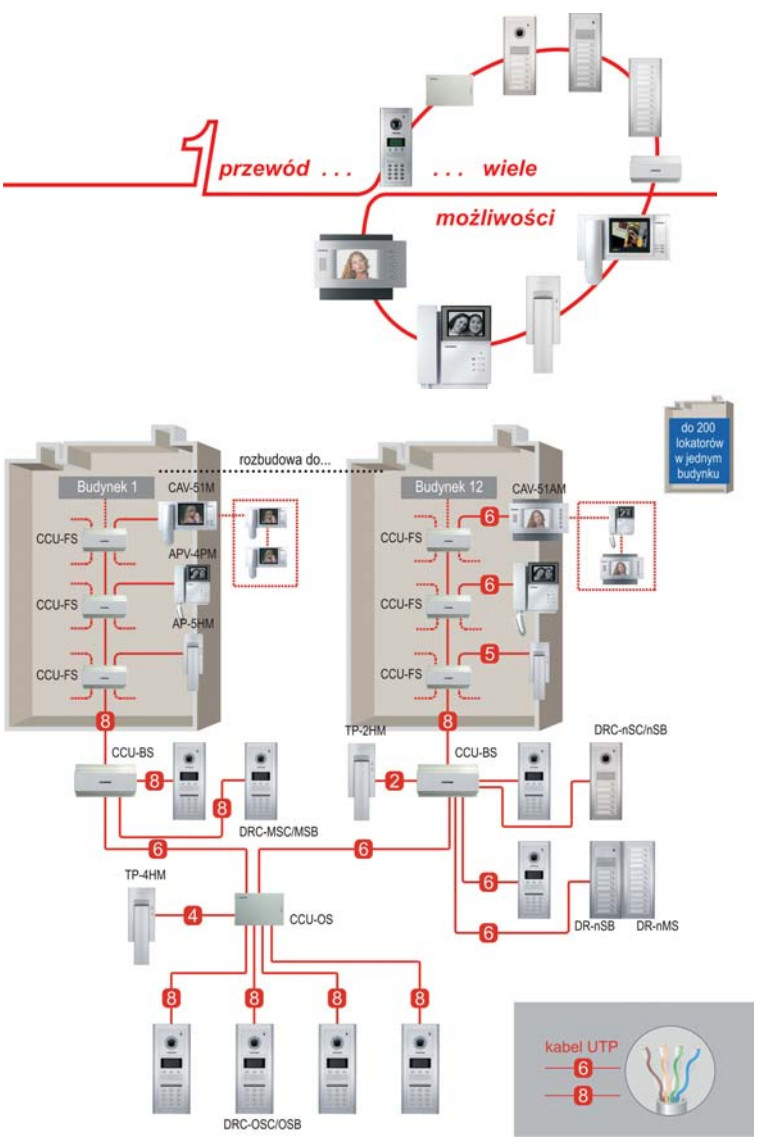


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna liczba obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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



Dystrybucja: GDE POLSKA

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

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

iSTAR Edge – Inteligentny kontroler IP

Produkt Software House® obsługujący 2 czytniki jest samodzielnym kontrolerem drzwi z własnym procesorem i bazą danych, współpracującym z systemem CCure, oferujący również niezależną pracę w istniejącej sieci i wiele zaawansowanych funkcji w konkurencyjnej cenie. Aby wykorzystać rosnącą popularność PoE (Power over Ethernet) w infrastrukturze sieci umożliwia zastosowanie opcjonalnego zasilania przez sieć.

Najważniejsze cechy i funkcje iSTAR Edge

- steruje i zasila wszystkie urządzenia kontroli dostępu w obrębie drzwi, redukując przez to koszty instalacji (przy zasilaniu PoE)
- umożliwia wiele opcji zasilania w tym wydajny, opcjonalny moduł zasilający Power over Ethernet (PoE) zawierający PoE (802.3af) i PoE Plus (802.3at)
- posiada bogate rozwiązanie zawierające antypassback i możliwość pracy w grupach jako peer-to-peer
- wewnętrzna pamięć umożliwia zapis i obsługę do 400000 kart
- wyposażony jest w pełny zestaw wejść/wyjść do obsługi 2 drzwi oraz dodatkowo opcjonalny moduł rozszerzeń I/O
- aktualizacja oprogramowania kontrolera możliwa bezpośrednio z serwera
- przez lokalny wyświetlacz LCD i diody LED dostarcza informacji o stanie uruchamiania i pracy kontrolera
- wbudowane 256-bitowe szyfrowanie sieci AES
- w pełni kompatybilny z C•CURE® v.10.0 i C•CURE® 9000 oraz innymi urządzeniami firmy Software House® w tym iSTAR Pro i iSTAR Ex

Parametry techniczne	
Wymiary (wys. x szer. x głęb.)	Obudowa: 305 x 305 x 101 mm ; Karta: 190 x 146 x 25 mm
Masa (z obudową)	4,2 kg
Zasilanie	12 V_{DC} lub 24 V_{DC} płyta główna – 400 mA; max 3,8 A 12 V_{DC} 3,1 A 24 V_{DC} dla wszystkich dołączonych urządzeń
Opcjonalnie PoE dla zasilanych urządzeń	PoE – 650 mA przy 12 V ; PoE Plus – 1700 mA przy 12 V
Podtrzymanie pamięci	4 baterie AA (żywotność 5 lat)
Pamięć wbudowana	64 MB RAM, 128 MB flash EEPROM podział pamięci dynamiczny pomiędzy danymi użytkowników, rejestracją zdarzeń i konfiguracją
Komunikacja sieciowa	jeden port 10/100Base-T
Obsługiwane czytniki	2 sztuki typu Wiegand i RM
Maksymalna odległość do drzwi	Wiegand : 150 m; RM: 1219 m
Wejścia	8 wejść nadzorowanych, tamper, awaria zasilania, niski poziom baterii, możliwość rozbudowy do 32 dodatkowych za pomocą modułów I8 RM
Wyjścia	4 konfigurowane przez przełączniki jako napięciowe lub zwarciowe

PR411DR – Kontroler dostępu dla jednego przejścia z możliwością pracy w trybie autonomicznym lub sieciowym

Charakterystyka:

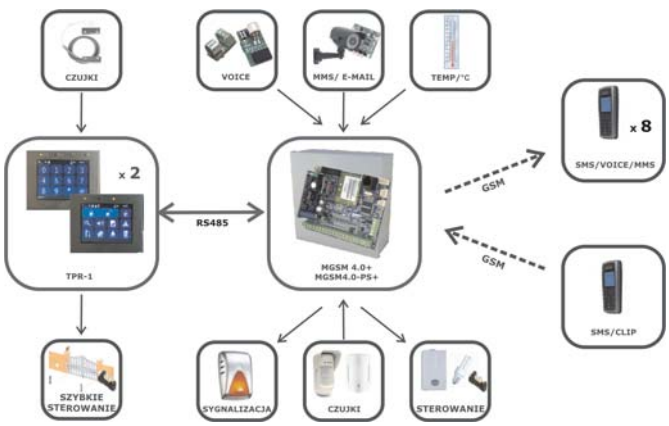
- Współpraca z jednym lub dwoma czytnikami pracującymi w formacie RACS (Roger) lub Wiegand
- Wbudowany zasilacz buforowy 1,5 A z obsługa akumulatora
- Zasilanie 18 V_{AC} lub 12V_{DC}
- Osiem programowalnych linii wejściowych NO/NC
- Dwa programowalne wyjścia tranzystorowe 1 A
- Jedno programowalne wyjście przekaźnikowe 1,5 A / 30V
- Jedno programowalne wyjście przekaźnikowe 1,5 A / 230V_{AC}
- Komunikacja przez RS485
- Dowolna topologia magistrali komunikacyjnej
- 1000 użytkowników w systemie
- Obsługa dodatkowych użytkowników typu „gość" definiowanych indywidualnie na każdym kontrolerze (możliwość wykorzystania w systemach hotelowych)
- 99 harmonogramów czasowych (*)
- 250 grup dostępu (*)
- 250.000 zdarzeń w buforze (*)
- Lokalny anti-passback
- Globalny anti-passback (*)
- Globalne sterowanie stanem uzbrojenia z podziałem na strefy alarmowe (*)
- Możliwość dołączenia ekspandera we/wy typu XM-2
- Integracja z systemem alarmowym za pośrednictwem linii we/wy
- Tryby drzwi: Normalny, Zablokowane, Odblokowane i Warunkowo Odblokowane
- Tryby identyfikacji: Karta lub PIN, Karta i PIN, tylko Karta, Tylko PIN
- Szybkie programowanie (ok. 15 sekund na każdy kontroler w systemie)
- Szybka aktualizacja uprawnień użytkownika (ok. 3 sekund na każdy kontroler w systemie)
- Możliwość podziału systemu na podsystemy (maks. 250 podsystemów)
- Współbieżne konfigurowanie podsystemów (ilość podsystemów nie zwiększa czasu przesyłania ustawień)
- Obudowa z tworzywa sztucznego przystosowana do montażu na szynie DIN 35mm
- Znak CE

(*) – funkcje dostępne tylko w systemach wyposażonych w centralę CPR32-SE

Produkcja:
roger®
Roger Sp. j.
Gościszewo 59
82-400 Sztum, woj. pomorskie
tel. (55) 272 01 32, faks (55) 272 01 33
e-mail: roger@roger.pl
http://www.roger.pl

MGSM 4.0+/4.0-PS+ & TPR-1
Centrala alarmowa z komunikacją GSM sterowana panelem dotykowym (klawiaturą dotykową)

Centrala alarmowa MGSM 4.0+/4.0-PS+ wraz z panelem dotykowym TPR-1 i pozostałymi dedykowanymi urządzeniami to nowoczesna konstrukcja spełniająca wymagania najbardziej wymagających klientów. Wbudowany komunikator GSM pozwala na bezpośrednie przesyłanie informacji na telefony użytkowników i/lub stacji monitorowania. Ponadto zintegrowany moduł GSM pozwala na zdalne sterowanie systemem (czuwaniem) poprzez SMS-y. System pozwala także na sterowania urządzeniami (wyjściami) poprzez SMS-y lub sygnały CLIP. Centrala MGSM 4.0+ wyposażona jest w automatyczne funkcje monitorujące stan systemu.



Centrala dodatkowo może być rozbudowana o następujące urządzenia:

- panel dotykowy TPR-1, nowoczesna klawiatura do kontroli systemu „TouchPanel", z unikalnymi funkcjami i eleganckim wyglądzie
- moduł FGR-4 do przesyłania wiadomości MMS/E-MAIL ze zdjęciami z kamer przemysłowych, pozwalające na weryfikacje wideo stanu obiektu
- syntezer mowy VSR-2, pozwalający na przesłanie 16 komunikatów głosowych zawierających unikalne informacje o zdarzeniu (VOICE),
- syntezer mowy VSR-1, pozwalający na przesłanie komunikatu głosowego (VOICE),
- moduł audio AMR-1 (mikrofon), pozwalający na podsłuch obiektu (weryfikacja audio),
- czujnik temperatury TSR-1, służący do kontroli temperatury i funkcji termostatu,
- zasilacz systemowy PSR z mikroprocesorową kontrolą parametrów i akumulatora,
- zasilacz systemowy z wbudowanym sterownikiem radiowym PSR-RF, pozwala na sterowanie czuwaniem systemu i wyjściami przekaźnikowymi poprzez piloty radiowe.

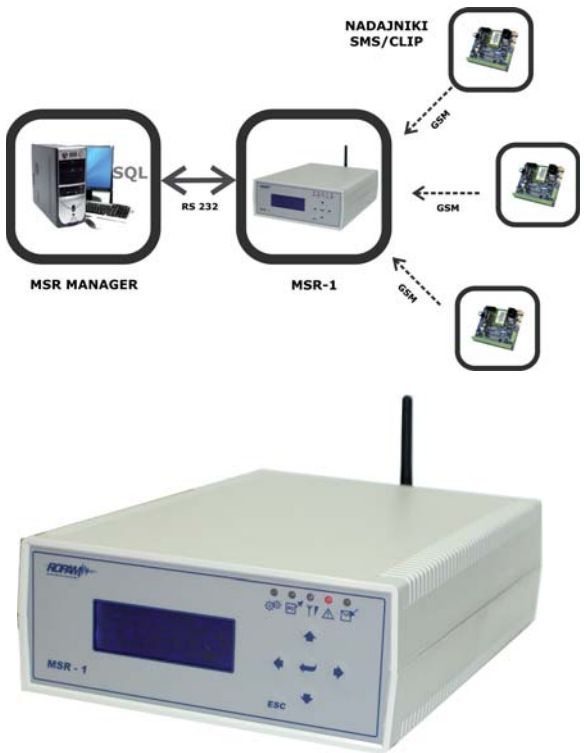
System alarmowy zbudowany z centrali alarmowej serii MGSM 4.0+/4.0-PS+, panelu dotykowego z kolorowym wyświetlaczem TPR-1 oraz innych urządzeń dodatkowych to idealne rozwiązanie dla obiektów mieszkalnych i małych obiektów komercyjnych. Intuicyjny i przejrzysty interfejs, powoduję że sterowanie systemem alarmowym jest intuicyjne i wyjątkowo proste. Panel dotykowy w połączeniu z modułami MGSM 4.0+/4.0-PS+ pozwala na zbudowanie w pełni funkcjonalnego systemu alarmowego. Przy połączeniu dwóch paneli otrzymujemy następującą konfigurację: 12 wejść, 10 wyjść, jedna strefa z czuwaniem nocnym oraz z wbudowaną komunikacją i sterowaniem GSM. Centrala MGSM 4.0+/4.0-PS+ pozwala ponadto na stworzenie prostych aplikacji automatyki domowej ze zdalną kontrolą poprzez sygnały SMS/CLIP. Elastyczne funkcje pozwalają ponadto na stosowanie centrali alarmowej w systemach, w których wykorzystuje się kontrolę sygnałów binarnych, temperaturę, wymagana jest weryfikacja wizualna a przesyłanie informacji jest w standardach SMS, VOICE, MMS, e-mail.

Z podstawowych właściwości systemu należy wyróżnić:

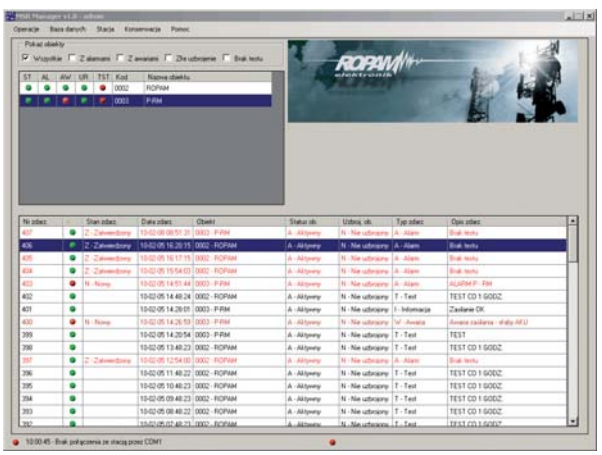
- 8 do 12 wejść do podłączenia czujek, urządzeń wyzwalających,
- 8 do 12 wyjść sterowanych, dedykowanych do sygnalizacji lub sterowania,
- wbudowany komunikator GSM z transmisją na 8 numerów telefonu,
- przesyłanie informacji o stanie systemu poprzez SMS,
- przesyłanie informacji głosowej (VOICE),
- przesyłanie wiadomości multimedialnej (MMS/E-MAIL),
- funkcja pomiaru temperatury i termostatu,
- funkcje kontroli połączenia,
- funkcje ograniczenia i kontroli kosztów.

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

Stacja monitorowania MSR-1 & MSR Manager



Stacja monitorowania MSR-1 wraz z oprogramowaniem MSR Manager to nowoczesne rozwiązanie dedykowane do monitoringu poprzez SMS / CLIP. System składa się z autonomicznego odbiornika MSR-1 w obudowie typu desktop oraz aplikacji bazodanowej do zarządzania sygnałami i obiektami. Odbiornik pozwala na odbiór sygnałów SMS/CLIP (CID CallerID) z modułów GSM marki Ropam lub innych zgodnych. Oprogramowanie to licencyjna aplikacja jednostanowiskowa pracująca w środowisku WINDOWS.



Odbiornik MSR-1

- autonomiczna konstrukcja pozwalająca na okresową pracę off-line
- port RS232 do komunikacji z MSR Manager
- lokalny bufor zdarzeń (500) podczas pracy off-line
- estetyczna obudowa z ABS typu 'desktop'
- duży podświetlany wyświetlacz LCD i klawiatura
- dodatkowa sygnalizacja LED i akustyczna
- zasilanie 230 V_{AC}
- wbudowane zasilanie awaryjne
- wbudowany przemysłowy modem GSM
- przystosowana do odbioru informacji nadawanych przez nadajniki GSM: SMS/CLIP
- możliwość podłączenia dużej ilości obiektów
- funkcja uaktualnienia oprogramowania (firmware)

Oprogramowanie MSR Manager

- licencja dla jednego stanowiska
- aplikacja bazodanowa (SQL)
- praca w środowisku WINDOWS
- łatwa instalacja i konfiguracja
- przyjazna obsługa i prezentacja zdarzeń
- wielopoziomowa struktura dostępu
- rozbudowane funkcje filtracji i przeszukiwania bazy danej
- funkcje eksportu ustawień
- funkcja tworzenia kopii zapasowych bazy danej
- możliwość szybkiej re-instalacji i odtworzenia bazy danej i ustawień
- małe wymagania sprzętowe

Przeznaczenie

System przeznaczony jest do monitoringu sygnałów alarmowych, technicznych, awaryjnych z nadajników GSM pracujących w standardzie SMS /CLIP. Rozwiązanie dedykowane jest do obsługi małych i średnich obiektów (do 1000 obiektów). Dzięki uniwersalnym funkcjom, elastycznemu oprogramowaniu szczególnie zalecane jest do monitoringu:

- systemów alarmowych i kontroli dostępu
- układów automatyki np. przepompownie, studnie
- systemów teletechnicznych
- serwerowni
- systemów awaryjnego zasilania np. USP-y, agregaty prądotwórcze
- sygnałów serwisowych
- ferm hodowlanych itp.

Producent:

Ropam Elektronik s.c.
Os.1000-lecia 6A/1
32-400 Myślenice

tel. (12) 379 34 47, tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
http://www.ropam.com.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

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

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

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

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

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

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

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

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

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

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

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

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

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

ADT Fire and Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 83 01
faks (22) 430 83 02
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

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

ALPOL Sp. z o.o.
ul. Ks. F. Ścigały 10
40-208 Katowice
tel. (32) 790 76 56
Infolinia 0 801 77 77 90
faks (32) 790 76 60
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

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

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

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

Al. Solidarności 15b, 25-323 **Kielce**
tel. (32) 720 39 82
faks (32) 790 76 94
e-mail: kielce@e-alpol.com.pl

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

ul. Grenadierów 13, 20-331 **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. Kutrzeby 16G, 61-714 **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

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

Zakład Produkcyjno-Usługowo-Handlowy
ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. (71) 363 17 53, faks wew. 7
e-mail: anma@anma-pl.eu
www.anma-pl.eu

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

ATLine Sp. J.
Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. (42) 657 30 80
faks (42) 655 20 99
e-mail: info@atline.pl
www.atline.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.pl

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

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

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
Tulipan Hause
02-672 Warszawa
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
ul. Garbary 5
86-050 Solec Kujawski
tel. (52) 387 36 58
tel. (52) 387 54 66, faks wew. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

CBC (Poland) Sp. z o.o.
ul. Krasińskiego 41A
01-755 Warszawa
tel. (22) 633 90 90
faks (22) 633 90 60
e-mail: handlowy@cbcpoland.pl
www.cbcpoland.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. Zatorska 36, 51-215 **Wrocław**
tel. (71) 340 0 209
faks (71) 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. (12) 260 1 395
faks (12) 260 1 396

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

CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 lok. U15
02-777 Warszawa
tel. (22) 855 00 17
faks (22) 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

Przedsiębiorstwo Usług Technicznych D-2 s.c.
K. Kolin, B. Czechowska
ul. Bukowa 1
40-108 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85
e-mail: dravisdravis@neostrada.pl
www.dravis.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: biuro@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
e-mail: dh-polska@dh-partner.com
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

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

ul. Wołczyńska 18, 60-003 **Poznań**
tel. (61) 863 82 08
faks (61) 866 64 16

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

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

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, 288 14 26, 278 18 86
faks (12) 278 48 91
e-mail: jablotron@jablotron.pl
www.jablotron.pl

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

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

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 518 84 00
faks (22) 812 62 12
e-mail: sales@ebs.pl
www.ebs.pl

ela-compil sp. z o.o.
ul. Słoneczna 15A
60-286 Poznań
tel. (61) 869 38 50-60
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. (22) 312 06 00
faks (22) 312 06 02
e-mail: elproma@elproma.pl
www.elproma.pl

ELTCRAC
Mirosław Gabzdyl, Marek Miękina Sp. J.
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60
faks (12) 292 48 65
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl

ELZA ELEKTROSYSTEMY
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 264 04 60
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl

EMU Sp. z o.o. Sp. k.
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. (22) 836 54 05, 837 75 93
tel. kom. 0 602 222 516
e-mail: warszawa@emu.com.pl

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

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

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

Przedstawicielstwo we Wrocławiu
tel. kom. 0 693 195 009
e- mail: factor.wr@factor.pl

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

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

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

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

ISM EuroCenter S.A.
ul. Wyczółki 71
02-820 Warszawa
tel. (22) 548 92 40
faks (22) 548 92 82
e-mail: ism@ismeurocenter.com
www.ismeurocenter.com

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

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 324 89 46
faks (32) 324 89 01
e-mail: systemy@kabe.pl
www.kabe.pl/1

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

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

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

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

NAPCO POLSKA
ul. Pszona 2
31-462 Kraków
tel. (12) 412 13 12
faks (12) 410 05 10
e-mail: napco@napco.pl
www.napco.pl

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

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 343 16 76, 341 98 54, 340 01 25
faks (71) 343 16 76
e-mail: obis@obis.com.pl
www.obis.com.pl

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

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

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

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

P.P.H. PETROSIN Sp. z o.o.
ul. Rysi Stok 8/2
30-237 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 Sp. z o.o.
ul. Irysowa 11
02-660 Warszawa
tel. (22) 831 15 35
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

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

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

RAMAR s.c.
U. Drogosz-Niemojewska, W. Niemojewska, M. Niemojewski
ul. Modlińska 237
03-120 Warszawa
tel./faks (22) 676 77 37, 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

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

ROPAM Elektronik s.c.
Os. 1000-lecia 6A/1
32-400 Myślenice
tel. (12) 379 34 47
tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.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
Czytniki dalekiego zasięgu
ul. Łączyny 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 314 69 50
e-mail: info@satie.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: 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: 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
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. (32) 291 86 17
tel./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

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

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

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

SCHNEIDER ELECTRIC BUILDINGS POLSKA Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10
faks (22) 313 24 11
e-mail:
SEPLBuildings.Poland@buildings.schneider-electric.com
www.schneider-electric.com/pl

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

ul. Rysia 1A
53-656 **Wrocław**
tel. (71) 711 09 19
faks (71) 711 09 20

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

SONY POLAND Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 25 73
tel. kom. (0) 600 206 117
faks (22) 520 25 77
e-mail: marcin.witkowski@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: sprint@sprint.pl
www.sprint.pl

Oddziały:
ul. Przemysłowa 15, 85-758 **Bydgoszcz**
tel. (52) 365 01 01
faks (52) 365 01 11

ul. Budowlanych 64E, 80-298 **Gdańsk**
tel. (58) 340 77 00
faks (58) 340 77 01

ul. Heyki 27C, 70-631 **Szczecin**
tel. (91) 485 50 00
faks (91) 485 50 12

ul. Canaletta 4, 00-099 **Warszawa**
tel. (22) 826 62 77
faks (22) 827 61 21

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.pl
www.aper.com.pl

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

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

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

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

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

ul. Inowrocławska 39 C, 53-649 **Wrocław**
tel. (71) 348 44 64
faks (71) 348 36 35
e-mail: wroclaw@spstrading.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 801 000 307
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.system7.pl
Internetowa Hurtownia Zabezpieczeń:
www.system7.biz

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

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, 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. (22) 516 97 97
faks (22) 516 97 91
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. (12) 39 89 900
faks (12) 39 89 901
e-mail: biuro@unicard.pl
www.unicard.pl

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

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
ADT Fire and Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	TAK	–	TAK
Alkam System	TAK	TAK	TAK	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	–
Atline	–	TAK	TAK	TAK	TAK
BOSCH	TAK	–	TAK	–	TAK
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	TAK	–	–	TAK
CBC Poland	TAK	–	TAK	–	TAK
CMA	TAK	TAK	TAK	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	TAK
D-2	–	TAK	TAK	TAK	–
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	TAK	TAK	TAK	TAK	TAK
DANTOM	TAK	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
DOM Polska	TAK	TAK	TAK	–	–
DPK System	–	–	TAK	TAK	TAK
Dyskam	TAK	TAK	–	TAK	TAK
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
ela-compil	TAK	–	TAK	–	TAK
El-Mont	–	TAK	–	TAK	–
Elproma	–	TAK	TAK	TAK	–
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	–	TAK	–	TAK	TAK
Emu	–	–	TAK	–	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	–	TAK	TAK	TAK	–
GDE Polska	–	–	TAK	–	TAK
HSA	–	–	TAK	–	–

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	TAK	TAK	–	TAK
KABE	–	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	–
Laskomex	TAK	TAK	TAK	–	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	TAK	TAK	TAK	–
NAPCO	–	–	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	TAK
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	TAK	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	–	TAK	TAK	TAK
RISCO	TAK	–	TAK	–	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	–
SATIE	TAK	–	TAK	TAK	–
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	–	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	–	–	TAK	–	–
Sony	TAK	–	–	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	TAK	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
ADT Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	TAK	TAK	TAK	–	–	TAK	–	TAK	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	TAK	TAK	–	TAK	–	–	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	–	TAK	–	–	TAK	–	TAK	–	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
bt electronics	–	–	TAK	–	–	–	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	–	–	–
CMA	TAK	–	–	–	–	–	TAK	–	–
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-2	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	–	–	TAK	TAK
DANTOM	TAK	TAK	TAK	TAK	–	–	–	TAK	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	–	–	–	–	–	–	–	–
Dyskam	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	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	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	–	–	TAK	–
FES	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	TAK	–	–
HSA	TAK	TAK	TAK	TAK	–	–	–	TAK	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	–	–	–	–	TAK	–	–
Janex International	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Laskomex	–	TAK	TAK	–	–	–	–	TAK	–
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	TAK	–	–	–	–	–
Nuuxe – Radioton	–	TAK	–	–	–	TAK	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	konserwacja i serwis zabezpieczeń mechanicznych								
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	–	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RISCO	TAK	–	TAK	–	–	TAK	TAK	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	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
Schneider Electric Buildings Polska	–	TAK	TAK	–	–	TAK	–	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Technokabel	TAK	TAK	TAK	TAK	TAK	–	TAK	–	TAK
UNICARD	TAK	TAK	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Adam Rosiński
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

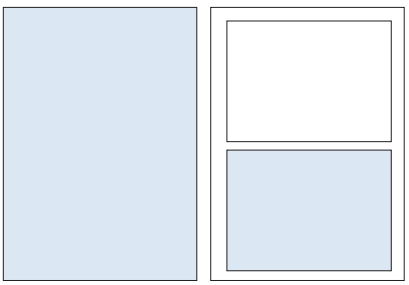
Spis teleadresowy:

jednorazowy wpis	70 zł

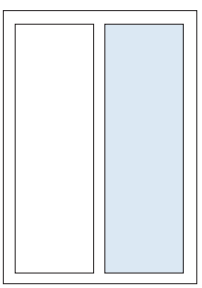
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

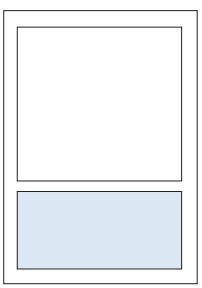
Podane ceny nie uwzględniają podatku VAT (22%)

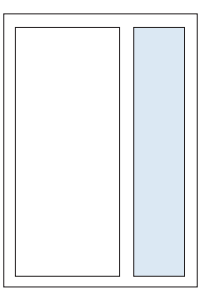
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej **http://www.zabezpieczenia.com.pl** w dziale **Reklama**

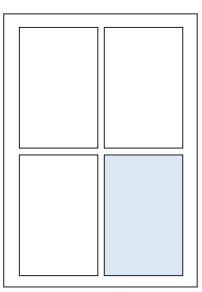

cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)


1/2 strony (83 x 260 mm)


1/3 strony (170 x 80 mm)


1/3 strony (54 x 260 mm)


1/4 strony (83 x 125 mm)

Spis reklam

Kamera kompaktowa z IR
BE4815PVR

CNB TECHNOLOGY Inc.

Kamera kopułkowa wandaloodporna z IR
V2810PVR

CNB TECHNOLOGY Inc.

CNB Technology jest wiodącym na świecie producentem kamer telewizji dozorowej z siedzibą w Korei Południowej. Od pierwszego dnia powstania firmy, niezmiennie do dziś, głównym założeniem jest inwestowanie w wykwalifikowaną kadrę inżynierów i nowe technologie, co przekłada się na bardzo wysoką niezawodność oraz szeroka gamę produktów. Jednym z ostatnich osiągnięć inżynierów z CNB jest stworzenie własnych układów scalonych DSP (przetwarzających obraz z przetwornika kamery) charakteryzujących się wiernym, naturalnym odwzorowaniem barw i szczegółów.

Kamera BE4815PVR

- kolorowa kamera dzień/noc
- przetwornik 1/3" Sony Super HAD
- wysoka rozdzielczość 550 TVL
- przełącza się w tryb b/w
- wyposażona w mechanicznie odsuwany filtr IR - TDN(ICR)
- czułość 0,3 lx (kolor), 0,008 lx (DSS 32 ramki), 0,00 lx (IR LED włączone)
- obiektyw 3,8÷9,5 mm DC
- OSD
- AGC, BLC, AWB, D/N, Flickerless
- cyfrowy zoom
- zasilanie dualne 12VDC/24VAC
- wbudowana grzałka i wentylator
- obudowa przystosowana do montażu do ściany

Kamera V2810PVR

- kolorowa kamera dzień/noc
- przetwornik 1/3" Sony Super HAD II
- wysoka rozdzielczość 550 TVL
- przełącza się w tryb B/W
- wyposażona w mechanicznie odsuwany filtr IR - TDN (ICR),
- czułość 0,3 lx (kolor), 0,1 lx (B/W), 0,0003 lx (DSS)
- obiektyw 2,8÷10,5 mm DC
- OSD
- AGC, BLC, D/N, DSS, SDNR, Flickerless, Eclipsa, zoom – regulacja przez OSD
- detekcja ruchu, strefy prywatności, funkcja mirror, wyostrzanie obrazu
- zasilanie 12V DC
- obudowa kopułkowa o średnicy 100mm, pozwalająca na montaż podwieszany do sufitu oraz w suficie podwieszanym

CNB TECHNOLOGY Inc.

importer i dystrybutor:

GDE POLSKA
Włosań, ul. Świątnicka 88, 32-031 Mogilany
tel. 12 256 50 25, 12 256 50 35, fax 12 270 56 96
e-mail: biuro@gde.pl, www.gde.pl, www.cnbtec.pl

Potrzebuję.....

mieć moje własne ID,
teraz, od razu, kiedy jest
mi potrzebne.

HID stwarza ci możliwość...

wyprodukowania kart ID w twoim własnym przedsiębiorstwie.

Technologie HID znacznie zmniejszają czas i koszt produkcji i umożliwiają większą kontrolę. Bez komplikacji, bez czekania... Najwyższej jakości karty, szeroki zakres technologii dostosowanych do indywidualnych potrzeb. Funcjonalność i bezpieczeństwo. Fargo umożliwia Ci kontrolowanie Twojego bezpieczeństwa dostarczając ekonomiczne i nowoczesne rozwiązania technologiczne.

HID

Chcąc stworzyć swój identyfikator, skontaktuj się z **hidglobal.com/cardissuance/Zab**