CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(118)/2017

ZABEZPIECZENIA

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

W NUMERZE:

Najlepsze rozwiązanie do obserwacji tuneli

NXM36 HiPoE

PoE IP66 IP68 IP69

Odporna na korozję obudowa NXM36 Hi-PoE ułatwia instalację kamer IP w trudnych warunkach środowiskowych. Zarówno kamera jak i grzałka systemu usuwającego wilgoć są zasilane metodą High Power PoE za pośrednictwem kabla Ethernet.

Wyposażenie dodatkowe stanowi wycieraczka przedniej szyby ze spryskiwaczem. Obudowa NXM36 może być zainstalowana na głowicy uchylno-obrotowej NXPTH, również wykonanej ze stali nierdzewnej.

VIDEOTEC

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy since 1986

RACS 5

System kontroli dostępu

- Wieloprzejściowe kontrolery dostępu serii MC
- Skalowalne oprogramowanie zarządzające VISO w architekturze klient – serwer
- Plikowa lub serwerowa baza danych w technologii MSSQL
- Bezpieczna komunikacja szyfrowana AES 128 CBC
- Funkcje automatyki budynkowej
- Integracja sprzętowa z systemem alarmowym
- Monitorowanie w trybie tekstowym i graficznym
- Integracje CCTV: Hikvision, Dahua
- Możliwość podziału systemu na zarządzane indywidualnie części

Rozszerzono ofertę systemu RACS 5 o zestawy kontroli dostępu

Wysoka niezawodność i funkcjonalność potwierdzona w tysiącach wdrożonych z sukcesem instalacji w Polsce i za granicą.

roger®

SPIS TREŚCI

Nowości produktowe w systemach telewizji dozorowej i monitoringu

Analiza obrazu prosta jak nigdy dotąd
dzięki rejestratorom NOVUS z serii 6000

Rejestratory IP NOVUS z **serii 6000** we współpracy z kamerami IP z **serii 3000** z funkcjami inteligentnymi umożliwiają skorzystanie z funkcji analizy obrazu, takich jak *wykrywanie obiektów*, *detekcja sabotażu*, *przekroczenie linii* oraz *naruszenie strefy*. Wszystkie wymienione funkcje, dostępne do tej pory wyłącznie jako autonomiczne funkcje kamer, są teraz w pełni konfigurowalne poprzez menu ustawień rejestratora. Ich konfiguracja jest przesyłana automatycznie do kamer, więc nie jest wymagany komputer do konfigurowania kamer za pomocą przeglądarki internetowej.

Dla pojedynczej kamery możemy zdefiniować funkcję wykrywania sabotażu oraz jedną z pozostałych funkcji analizy obrazu. Dzięki funkcji *Sabotaż* rozróżniane i wykrywane są następujące zdarzenia: zmiana obserwowanej sceny, rozmycie obrazu, błąd koloru. W przypadku funkcji *Wykrywanie obiektu* algorytm analizuje zarówno zniknięcie, jak i pozostawienie obiektu. Funkcja *Przekroczenie linii* umożliwia zdefiniowanie do czterech linii w pamięci kamery, przy czym zawsze tylko jedna jest aktywna. Podobnie jest w przypadku funkcji *Naruszenie strefy*.

W przypadku wszystkich powyższych funkcji można podjąć akcję alarmową. Do wyboru mamy następujące opcje: zapis zrzutu ekranu, aktywacja wyjścia alarmowego w kamerze, ustawienie kamery w zdefiniowany sposób, włączenie brzęczyka, wyświetlanie obrazu z kamery na pełnym ekranie lub wysłanie wiadomości e-mail wraz z załączonym zdjęciem ukazującym zdarzenie.

Bardzo wartościowym i docenianym przez klientów uzupełnieniem akcji alarmowej jest włączenie serwera typu push on w rejestratorze. Dzięki temu w telefonie komórkowym, w zakładce *powiadomienia*, wyświetlane są informacje o zaistniałych zdarzeniach, gdy program SuperLivePlus jest wyłączony. Umożliwia to szybką reakcję na zdarzenie, które zarejestrowano w obiekcie. Po potwierdzeniu powiadomienia automatycznie uruchamia się oprogramowanie wyświetlające w trybie na żywo obraz z kamery, która wywołała alarm. Funkcja jest aktywna zgodnie z zaprogramowanym uprzednio harmonogramem.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

NOVUS® 6000 SERIA IP

8 HDD H.265 4K HDMI

MOŻLIWOŚĆ INSTALACJI DO 8 DYSKÓW WEWNĄTRZ!

DUŻO WIĘCEJ MIEJSCA NA TWOJE ARCHIWUM

W REJESTRATORZE NVR-6332-H8

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Axis Communications przedstawia nową wersję Zipstream z obsługą kamer o polu widzenia 360° i rozdzielczości 4K

Firma **Axis Communications** przedstawiła nową wersję kompresji metodą **Zipstream**, która jest w stanie sprostać wymaganiom dotyczącym transferu i przechowywania danych przez kamery panoramiczne o 360-stopniowym polu widzenia oraz inne urządzenia tworzące obraz o rozdzielczości 4K. Firma wprowadziła do swojej oferty dwie nowe kamery kopułkowe spełniające te wymagania.

Wymagania klientów dotyczące systemów dozoru wizyjnego mogą wydawać się sprzeczne – oczekują poprawy jakości, rozdzielczości i pola widzenia kamer, a jednocześnie redukcji kosztów wykorzystania łączy i przechowywania danych. Axis Communications uwzględnia te potrzeby poprzez ciągłe poprawianie kompresji obrazu metodą Zipstream, która powstała specjalnie z myślą o wizyjnych systemach dozorowych marki AXIS. Zipstream umożliwia zmniejszenie potrzebnej przepustowości sieci oraz wymaganej przestrzeni dyskowej średnio o 50% bez ryzyka utraty ważnych szczegółów rejestrowanego obrazu.

– *Przechowywanie danych i przepustowość łącz stanowią istotny element całkowitych kosztów wizyjnego systemu dozorowego. Nasza metoda Zipstream pozwala na zaspokojenie specyficznych potrzeb branży zabezpieczeń – pozwala na zminimalizowanie wymagań bez utraty szczegółów rejestrowanego obrazu* – powiedział Jan T. Grusznic, Sales Engineer/Technical Trainer w firmie Axis Communications. – *Cieszymy się, że teraz Zipstream działa także z kamerami panoramicznymi i Ultra HD.*

Firma zaprezentowała dwie nowe kopułkowe kamery sieciowe AXIS M3047-P i AXIS M3048-P, które wykorzystują ulepszoną metodę Zipstream, dzięki czemu są w stanie wytwarzać obraz w 360-stopniowym polu widzenia, a jednocześnie ich ceny są przystępne.

Nowe kamery wyglądają atrakcyjnie, mają mniejsze rozmiary, są płaskie i nie mają dodatkowej kopuły nad obiektywem. Dzięki temu nie ma ryzyka pojawienia się refleksów w kopule, a kamery są bardziej dyskretne. Jako wyposażenie dodatkowe oferowane są odporne na uszkodzenia obudowy do obu modeli. Dostępne są wersje w kolorze czarnym. Kamery realizują zarówno wewnętrzną, jak i zewnętrzną korekcję zniekształceń perspektywy obrazu panoramicznego. Płynna obróbka obrazu w pełnym, 360-stopniowym polu widzenia może być w prosty sposób wykonana z wykorzystaniem AXIS Camera Station, a także innych systemów do zarządzania obrazami, zarówno podczas podglądu na żywo, jak i na wcześniej nagranych materiałach.

Rozdzielczość matrycy wynosi 6 megapikseli w przypadku kamery AXIS M3047-P i 12 megapikseli w przypadku kamery AXIS M3048-P. Oba urządzenia zapewniają pełnoekranowy obraz o doskonałej jakości, a także korekcję ostrości i wysoką światłoczułość.

– Połączenie nowych kamer kopułowych o polu widzenia 360 stopni z najnowszą wersją kompresji Zipstream daje naprawdę opłacalne rozwiązanie dla klientów – zapewnia kompleksową obserwację monitorowanego obszaru z zachowaniem wysokiego poziomu szczegółowości panoramicznego obrazu – powiedział Jakub Kozak, Sales Manager – Poland, Ukraine, Baltics, w Axis Communications.

Premiera nowej wersji Axis Zipstream oraz kamer panoramicznych AXIS M3047-P i AXIS M3048-P miała miejsce podczas IFSEC International 2017. Obie kamery są dostępne u dystrybutorów produktów firmy Axis Communications.

Bezpośr. inf.
Axis Communications

Zipstream wyłączony | **2881 kbit/s**

Axis Communications wprowadza radar
do systemów zabezpieczeń

Axis Communications wprowadza do oferty urządzenia wykorzystujące radarowe metody wykrywania obiektów, które pozwalają wyeliminować wiele nieuzasadnionych alarmów podczas ochrony otwartych przestrzeni. Zaprojektowano je w taki sposób, by były łatwe do zainstalowania oraz by istniała możliwość zintegrowania ich z istniejącymi systemami zabezpieczeń.

Axis Communications, globalny lider w branży wizyjnych systemów dozorowych, wprowadza na rynek nowe urządzenie – radar **AXIS D2050-VE**. Radarowa metoda wykrywania obiektów umożliwia precyzyjne i wiarygodne monitorowanie dużych obszarów oraz wykrywanie poruszających się obiektów niezależnie od pogody czy warunków oświetleniowych. Radary AXIS D2050-VE mają uzupełniać kamery z funkcją wykrywania ruchu i mogą być wykorzystywane razem z urządzeniami PTZ do śledzenia przemieszczających się obiektów. Umożliwiają skuteczne monitorowanie dużych przestrzeni w przeciwieństwie do kamer termowizyjnych, które są przeznaczone do zabezpieczania wydzielonych obszarów w ramach ochrony perymetrycznej. Stworzono je z myślą o instalacjach przemysłowych średniej wielkości. Mogą być łatwo zintegrowane z innymi urządzeniami Axis i oprogramowaniem do zarządzania wizyjnymi systemami dozorowymi (VMS) – także innych producentów.

Odporne na uszkodzenia mechaniczne i nadające się do użytku na zewnątrz urządzenie AXIS D2050-VE może w czasie rzeczywistym dostarczać informacji o położeniu, prędkości i kierunku przemieszczania się, a także wielkości poruszającego się obiektu. Dzięki dużemu zasięgowi, który jest wielokrotnie większy od zasięgu pasywnych czujek podczerwieni, zapewnia większy obszar obserwacji i jednocześnie minimalizuje liczbę nieuzasadnionych alarmów wywoływanych przez owady i małe zwierzęta, cienie czy odbicia światła. Detektor ruchu może być skonfigurowany tak, aby włączał rejestrację obrazów dostarczanych przez kamery, głośnik sieciowy czy reflektor, który oświetli podejrzany obiekt.

Czujka radarowa Axis może być używana jako samodzielny element lub jako część systemu dozorowego. Dzięki otwartemu interfejsowi jest kompatybilna z kamerami Axis i można ją łatwo zintegrować z oprogramowaniem Axis Camera Station i Axis Camera Management, a także z innymi wizyjnymi systemami dozorowymi.

– *Radar jest istotnym dopełnieniem systemów zabezpieczeń, ponieważ zapewnia skuteczne wykrywanie obiektów na chronionym obszarze. Wykrywa obiekty ruchome z dużą dokładnością i redukuje liczbę nieuzasadnionych alarmów* – wyjaśnia Jakub Kozak, Sales Manager Poland, Ukraine, Baltics w Axis Communications. – *W porównaniu z prostymi detektorami ruchu system AXIS D2050-VE udostępnia dodatkowe informacje o wykrytych obiektach, które umożliwiają ich automatyczne śledzenie za pomocą kamer PTZ. Klienci mogą teraz łatwo dodać sprawdzoną, radarową metodę wykrywania obiektów do już istniejących lub dopiero powstających systemów zabezpieczeń.*

AXIS D2050-VE jest dostępny u dystrybutorów produktów firmy Axis Communications od października 2017 roku.

Bezpośr. inf.
Axis Communications

Uchwyć każdy szczegół, który ma znaczenie

Dahua prezentuje linię kamer - Machine Vision

- 20 letnie doświadczenie w pozyskiwaniu, przetwarzaniu i rozpoznawaniu obrazów
- Darmowe i łatwe w użyciu SDK z zestawem instrukcji bibliotek API dostępnych dla różnych języków programowania
- Wysoka niezawodność produktu potwierdzona testami jakości
- Nasze działy techniczne na całym świecie zapewniają dostosowanie zastosowań kamer do indywidualnych potrzeb Klienta, oraz pełne wparcie serwisowe
- Bogata oferta produktów zapewniająca skanowanie obszaru / skanowanie linii (GigE lub USB3.0) z szerokim spektrum obiektywów przy niskich zniekształceniach

ISO 9001:2000

www.dahuasecurity.com/pl

Dahua Technology Poland Sp. z o.o.
ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

MIC IP starlight 7000i firmy Bosch

kamery do zadań specjalnych

Kamery ruchome **MIC IP starlight 7000i** zaprojektowano z myślą o stosowaniu ich w niemal każdych warunkach środowiskowych. Zastosowano w nich funkcje **Intelligent Video Analytics** i **Starlight**, a także wyposażono je w wyjątkowo wytrzymałe obudowy. Dodatkowo można je wyposażyć w opcjonalny promiennik, który pozwala tworzyć obraz w całkowitej ciemności, nawet na odległość 450 m. Kamery MIC IP starlight 7000i dokonują analizy treści obrazu nawet pod-

czas obracania, zmiany nachylenia lub przybliżania obrazu. Po wykryciu poszukiwanego obiektu lub osoby powiadamiają operatora lub uruchamiają funkcję Intelligent Video Tracking. Kamery MIC IP starlight 7000i mają wysoką odporność na uderzenia, wstrząsy i ekstremalne warunki pogodowe. Dzięki temu dostarczają istotnych danych nawet w trudnych warunkach środowiskowych.

Bezpośr. inf.
Bosch Security Systems

Obudowy do kamer

pracujących w środowiskach agresywnych chemicznie

Obudowy **NXM36 Hi-PoE** zostały opracowane przez firmę **Videotec** z myślą o instalacjach wykonywanych w miejscach, w których są one narażone na korozję, takich jak tunele drogowe, zakłady chemiczne i petrochemiczne, morskie platformy wiertnicze, morskie instalacje okrętowe i portowe. Powłoka zewnętrzna tych obudów jest wykonana ze szlifowanej stali nierdzewnej spełniającej wymagania AISI 316L dotyczące odporności na korozję. Obudowy spełniają wymagania dotyczące czterech klas szczelności – IP66, IP67, IP68 oraz IP69. Zapewnia to ich całkowitą odporność na zanieczyszczenia oraz na zanurzanie w wodzie na głębokość do 40 m.

Urządzenia zainstalowane w obudowach NXM36 Hi-PoE, w tym kamery, grzałki i zespoły usuwające wilgoć, mogą być zasilane metodą PoE lub Hi-PoE, dzięki czemu bardzo upraszcza się okablowanie. Tym samym redukowane są koszty instalacji punktów kamerowych.

Dodatkowym wyposażeniem obudów NXM36 Hi-PoE są wycieraczki ze spryskiwaczem, które umożliwiają łatwe usuwanie zanieczyszczeń z przedniej szyby. Obudowy NXM36-Hi-PoE mogą być instalowane na głowicach uchylno-obrotowych NXPTH spełniających te same wymagania środowiskowe, więc można łatwo stworzyć zdalnie sterowane punkty kamerowe przeznaczone do pracy w środowiskach agresywnych chemicznie.

Dodatkowe informacje są dostępne na stronie www.videotec.com.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

Obraz jest najważniejszy
nowa kamera GenSTAR w ofercie CBC

12MP bullet to kolejna nowość uzupełniająca popularną serię kamer **Ganz IP GenSTAR**. **ZN8-BB12M412-N** ma obiektyw typu motor-zoom o ogniskowej regulowanej w zakresie od 4.1 mm do 12.8 mm. Sterowanie obiektywem jest realizowane dzięki zastosowaniu mechanicznego napędu optycznych elementów obiektywu. Funkcja ta jest szczególnie doceniana przez instalatorów, ze względu na krótszy czas regulacji kamery, a także w przypadku zastosowania kamery w miejscu, gdzie wymagana jest okresowa zmiana zakresu pola widzenia. Kamera ma cyfrowe systemy WDR oraz HLC realizujące funkcje umożliwiające przyciemnienie silnie oświetlonych fragmentów pola widzenia w celu zwiększenia wyrazistości obrazu. SMART-IR umożliwia dostosowanie natężenia światła z promiennika IR, emitowanego przez trzy niezależne sekcje diod IR-LED, w celu uniknięcia efektu prześwietlenia obiektów znajdujących się w pobliżu kamery, a funkcja ROI (ang. *Region of Interest*) umożliwia selektywną zmianę jakości obrazu w uprzednio określonych, priorytetowych obszarach obserwowanej sceny, co ma realny wpływ na ograniczenie objętości nagrań i potrzebnego miejsca w fizycznej pamięci masowej. Możliwość dopasowania pola widzenia do sceny charakteryzującej się znaczną dysproporcją pomiędzy wysokością i szerokością obrazu (czyli tzw. tryb korytarzowy) to kolejna cecha wyróżniająca tę kamerę. Serię GenSTAR uzupełniają kamery w obudowie IK10.

Bezpośr. inf. CBC Poland
www.cbcpoland.pl

Ganz CORTROL
oprogramowanie VMS klasy Enterprise

Skalowalność, uniwersalność i prostota to cechy najnowszego oprogramowania **VMS Ganz CORTROL** przeznaczonego do centralnego zarządzania. System jest dostępny w trzech wersjach – **Prime, Premiere** oraz **Global** – i oferuje wiele zaawansowanych funkcji zapewniających bardzo wydajny nadzór wizyjny. Oprogramowanie obsługujące kodeki H.264, H.265, MJPEG i MPG4 ma intuicyjny interfejs użytkownika oraz gwarantowaną wydajność. Dzięki centralnej strukturze hierarchicznej oraz wielu specjalistycznym modułom wersja Global jest przeznaczona do systemów CCTV o rozległej i rozproszonej architekturze. Do kluczowych zalet oprogramowania systemowego CORTROL możemy zaliczyć 64-bitowy rdzeń, gotowość do obsługi strumieni wizyjnych o rozdzielczości 4K oraz 8K oraz możliwość ich nagrywania i odtwarzania, pełną kontrolę i automatyzację procesu nadzoru wizyjnego za pomocą menedżera zdarzeń, zdalny dostęp za pośrednictwem aplikacji mobilnych, możliwość tworzenia własnych widoków oraz E-map i Geo-map, możliwość dodania wielu serwerów w jednej aplikacji klienckiej, funkcję strumieniowania obrazów i dwukierunkowej komunikacji za pomocą telefonu komórkowego, ciągłe monitorowanie stanu wszystkich serwerów i centralne zarządzanie pracą awaryjną (ang. *failover*), replikację danych archiwalnych, strumieniowanie RTMP (np. do strony WWW lub portalu YouTube), zaawansowane funkcje wyszukiwania materiału wizyjnego oraz wbudowany serwer WWW z multicastingiem. CORTROL umożliwia też identyfikację numerów rejestracyjnych pojazdów i identyfikację twarzy, ma wbudowany silnik Deep Learning VCA, a dzięki zestawowi API/SDK zapewnia możliwość integracji z innymi systemami VMS.

Bezpośr. inf. CBC Poland
www.cbcpoland.pl

Rejestratory sieciowe firmy Dahua Technology

Rejestratory sieciowe (NVR) firmy **Dahua Technology** są zintegrowane z detektorami zewnętrznymi wykorzystującymi protokół IP firmy GJD Manufacturing Limited. Integracja pozwala użytkownikom na kolejny krok w dziedzinie podnoszenia poziomu bezpieczeństwa. Detektory IP D-TECT i oświetlacze IP Clarius PLUS zostały zintegrowane z rejestratorami sieciowymi z serii NVR6XXX-4KS2 firmy Dahua.

Otwarta struktura rejestratorów umożliwia dostęp wielu użytkownikom i jest kompatybilna ze standardem ONVIF 2.4, dzięki czemu umożliwia współpracę z dowolnymi kamerami IP zgodnymi ze specyfikacją ONVIF.

Rejestratory umożliwiają inteligentną analizę treści obrazów, która pozwala na automatyczne wykrywanie osób i poruszających się obiektów, a także innych, z góry ustalonych zdarzeń (wykrywanie porzuconych lub znikających obiektów, wtargnięć, twarzy, liczenie osób).

Integrację osiągnięto poprzez włączenie interfejsu API GJD do specjalnego oprogramowania, które umożliwia weryfikację przyczyn alarmów z detektorów i korelowanie ich z funkcjami rejestratora.

Aby oferować coraz lepsze produkty i rozwiązania swoim klientom na całym świecie, firma Dahua Technology stale inwestuje w badania i rozwój oraz współpracuje z innymi firmami o globalnym zasięgu działania. Dahua Technology zamierza nadal dbać o jakość i innowacyjność.

Bezpośr. inf. Dahua Technology

Współpraca firm
Dahua Technology i QNAP

Firma **Dahua Technology**, czołowy dostawca wizyjnych systemów dozorowych, ogłosiła, że kamery IP z serii **Eco Savvy 3.0**, kodujące obrazy zgodnie z metodą H.265, od teraz są kompatybilne z pamięciami masowymi **QNAP NAS**. Aplikacje QNAP integrują wszechstronne funkcje wizyjnych systemów dozorowych z systemem NAS, zapewniając użytkownikom integrację bazy danych z systemem dozoru wizyjnego.

Dahua Technology jest jednym z najbardziej wszechstronnych producentów kamer w branży. Dzięki integracji z QNAP NAS klienci uzyskają bardziej kompleksowe funkcje, które spełniają wymagania wielu użytkowników.

– *Otwartość, integracja i wprowadzanie innowacji jest naszą dewizą* – powiedział Daniel Chau, dyrektor marketingu w firmie Dahua Technology. – *Jesteśmy otwarci na współpracę z partnerami, takimi jak QNAP, w celu tworzenia kompleksowych rozwiązań dla klientów. Doceniamy siłę naszych relacji i spodziewamy się wzrostu zapotrzebowania na systemy dozorowe wykorzystujące chmurę obliczeniową.*

Kamery Dahua Eco-Savvy 3.0 realizują funkcje wykrywania ludzi oraz inteligentnego śledzenia obiektów. Mają wiele inteligentnych funkcji do wykrywania intruzów, w tym funkcje rozpoznawania twarzy, wykrywania wtargnięć etc. Kompresują obrazy metodą H.265. Dzięki doskonałym parametrom obiektywów i dużej precyzji pozycjonowania przy korzystaniu z funkcji *pan/tilt/zoom* kamery Dahua H.265 PTZ znajdują wiele różnorodnych zastosowań.

Więcej informacji na temat urządzeń Dahua można znaleźć pod adresem: http://www.dahuasecurity.com.

Bezpośr. inf. Dahua Technology

Nowe kamery wielosensorowe
firmy Hanwha Techwin

Hanwha Techwin wprowadza do oferty dwa nowe modele kamer wielosensorowych – 8-megapikselową **PNM-9080VQ** i bliźniaczą, 20-megapikselową **PNM-9081VQ.**

W obu urządzeniach wykorzystywana jest kompresja H.265 oraz H.264. Kamery są wyposażone w cztery moduły optyczne o rozdzielczościach 2 i 5 megapikseli. Moduły te są obsługiwane niezależnie od siebie. Realizowane są takie funkcje jak pozycjonowanie, stabilizacja żyroskopowa, zdalne sterowanie obiektywem itd. Kamery można dostosować do obserwacji w polu widzenia 360° lub w trybie 3+1 (trzy kamery na obwodzie koła i jedna patrząca centralnie w dół). Oba omawiane modele kamer mają funkcje analizy treści obrazu (dziesięć różnych algorytmów), a do ich obsługi wystarcza pojedynczy adres IP. Jest to możliwe dzięki portowi sieciowemu o przepustowości 1 GB/s oraz procesorowi WiseNet P umożliwiającemu jednoczesne wysłanie czterdziestu strumieni wizyjnych, z których każdy można konfigurować indywidualnie. W kamerach wykorzystana jest innowacyjna metoda transmisji WiseStream, która redukuje pasmo sieciowe nawet do 75% w stosunku do standardowej kompresji H.264.

Inne zalety tych kamer to sprawny system WDR o dynamice równej 150 dB w PNM-9080VQ i 120 dB w PNM-9081VQ, gniazda dla kart SD, obudowa o klasie szczelności IP66 z certyfikatem udarowym IK10, szeroki zakres temperatur pracy i dualne zasilanie (12 V_{DC}/HPoE).

Bezpośr. inf. Piotr Rogalewski
Hanwha Techwin

Łączność P2P
w nowych rejestratorach sieciowych Hanwha Techwin

W celu uzupełnienia popularnej serii tanich urządzeń **WiseNet Q** firma **Hanwha Techwin** wprowadza do oferty dwa nowe rejestratory sieciowe.

QRN-410 i **QRN-810** to urządzenia odpowiednio 4- i 8-kanałowe z kompresją H.265, H.264 oraz MJPEG. Prędkość zapisu do 50 Mbps (model 4-kanałowy) lub 100 Mbps (model 8-kanałowy) umożliwia rejestrację obrazu o rozdzielczości do 8 megapikseli z prędkością do 30 kl./s dla każdego z kanałów, przy pełnej obsadzie kamer. Wbudowane wyjście monitorowe i port USB pozwalają na stworzenie prostego w obsłudze i taniego stanowiska obsługi bez konieczności podłączania dodatkowego komputera. Nowością w obu modelach jest łączność w trybie P2P, która bardzo ułatwia i przyspiesza proces zestawiania połączenia sieciowego między rejestratorem a urządzeniem mobilnym. Procedura połączenia sprowadza się do uruchomienia rejestratora i zeskanowania kodu QR urządzeniem mobilnym. Istotna jest także funkcja ARB, czyli automatyczne przywracanie kopii zapasowej.

W przypadku awarii sieci i utraty łączności kamer z rejestratorem materiał wizyjny jest awaryjnie zapisywany na lokalnych kartach SD, a po przywróceniu połączenia automatycznie wysyłany do rejestratora.

Bezpośr. inf. Piotr Rogalewski
Hanwha Techwin

KaDe Premium Plus II

zintegrowane z rejestratorami IP marki NOVUS

Firma **AAT** wkrótce zaprezentuje finalną wersję programu **KaDe Premum Plus II** zintegrowaną z rejestratorami IP marki **NOVUS** (seria 6000, modele 4-, 8- i 16-kanałowe).

W nowym programie KaDe Premium Plus II zostało zaimplementowane SDK umożliwiające komunikację z rejestratorami z serii 6000 poprzez sieć IP. Nowa wersja programu KaDE, podobnie jak poprzednie, oferuje możliwość nawiązania połączenia z rejestratorami IP, pobrania listy kamer i powiązania ich z elementami systemu kontroli dostępu. Metodą „przeciągnij i upuść" można przypisać poszczególnym kamerom takie elementy jak kontrolowane drzwi oraz czujki dołączone do wejść linii dozorowych kontrolera. Jedna kamera może być powiązana z więcej niż jednym elementem.

Udogodnieniem w trybie monitorowania na żywo jest automatyczne wyświetlanie okna wizyjnego na pulpicie operatora stacji systemu KaDe Premium Plus II. Zawiera ono obraz z kamery powiązanej z elementem systemu, którego dotyczy ostatnie zdarzenie. Umożliwia to operatorowi szybką weryfikację sytuacji w obiekcie. Ponadto w zakładce *Raporty*, po wybraniu opcji *Zdarzenia* lub *Alarmy* z trybu monitorowania na żywo, również pojawia się okno wizyjne. Po wyszukaniu w nim zdarzenia lub alarmu wyświetlany jest strumień wizyjny z archiwum przechowywanego na dysku rejestratora. Zapis jest odtwarzany z kamery zainstalowanej w miejscu lokalizacji elementu zgodnie z czasem wystąpienia zdarzenia.

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING

Inteligentne funkcje rejestratorów AHD
marki NOVUS

Rejestratory **AHD 4 Mpx** obsługujące wszystkie dostępne na rynku standardy telewizji analogowej (AHD, CVI, TVI, Analog) wzbogacono w algorytmy inteligentnej analizy obrazu (VCA). Funkcje VCA zostały zaimplementowane w rejestratorach **NHDR-4M5316AHD** oraz **NHDR-4M5308AHD**. Dotyczą one jednego kanału AHD niezależnie od rodzaju sygnału dostarczanego przez kamery (algorytmy analizy są realizowane w rejestratorze). Dodatkowo w przypadku kamer sieciowych IP NOVUS z serii 2000 wszystkie kanały IP mają funkcje inteligentne (algorytmy analizy są realizowane w kamerach).

W przypadku funkcji *Naruszenie strefy* można zdefiniować do czterech stref detekcji. Zdarzenie alarmowe jest generowane w momencie przekroczenia granicy strefy przez obiekt poruszający się w określonym kierunku. Funkcja *Przekroczenie linii* pozwala wyznaczyć do czterech linii detekcji, a zdarzenie alarmowe jest generowane w momencie przekroczenia wyznaczonej linii przez obiekt poruszający się w określonym kierunku. W przypadku funkcji *Wykrycie obiektu* zdarzenie jest wywołane pojawieniem się obiektu w określonej strefie lub zniknięciem obiektu. W celu zmniejszenia liczby fałszywych zdarzeń zakres czasowy działania ww. funkcji może być ustalony za pomocą graficznego harmonogramu.

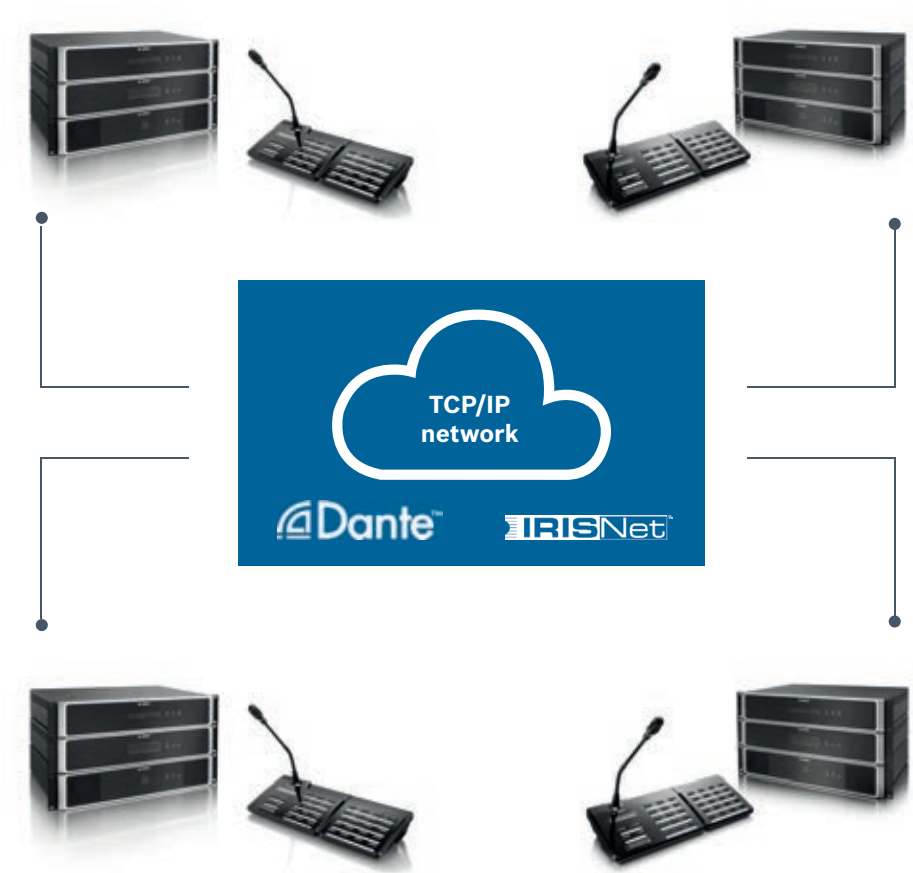
Wszystkie zdarzenia VCA są zapisywane w logach systemowych urządzenia, dzięki czemu w trybie odtwarzania można natychmiast obejrzeć odfiltrowane zdarzenia. Dodatkowo do powyższych zdarzeń można przypisać akcję alarmową, np. wyświetlenie obrazu na pełnym ekranie, włączenie sygnału dźwiękowego, wysłanie wiadomości e-mail lub wyświetlenie ikony zdarzenia.

W przypadku większości obiektów ww. funkcje mogą zautomatyzować proces nadzoru, uczynić go bardziej niezawodnym i odciążyć operatora systemu dozorowego.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Centrala dźwiękowego systemu ostrzegawczego PAVIRO

w wersji sieciowej



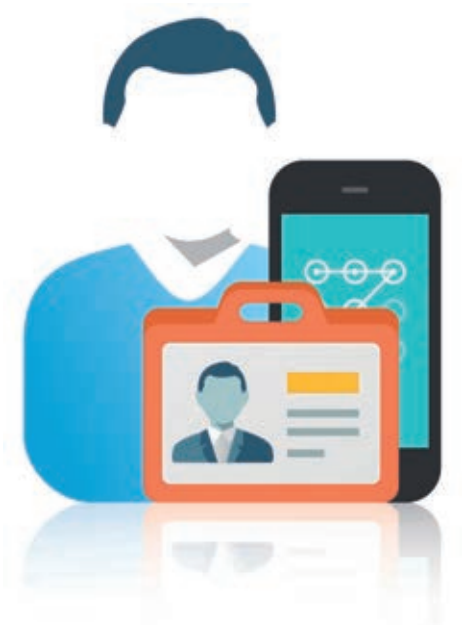
System nagłośnieniowy i dźwiękowy system ostrzegawczy **PAVIRO** firmy **Bosch** zawiera teraz nowe rozwiązania sprzętowe i programowe, które dzięki najnowocześniejszym rozwiązaniom sieciowym (IP) umożliwiają stosowanie go w większych instalacjach.

Dzięki wykorzystaniu sieci IP system PAVIRO stanowi wysoce elastyczne, niezawodne i bezpieczne rozwiązanie. Zapewnia najwyższą jakość odtwarzania dźwięku i minimalne czasy opóźnień. Ponadto za pośrednictwem sieci można zintegrować PAVIRO z innymi urządzeniami, takimi jak komputery PC czy laptopy, co umożliwia efektywną zdalną kontrolę i diagnostykę, a także stwarza możliwość konserwacji systemu przez Internet.

PAVIRO zawdzięcza pracę w sieci IP i komunikację nowemu modułowi interfejsu sieciowego Dante (OM-1) firmy Bosch. Umożliwia on stworzenie 16-kanałowej sieci akustycznej Dante łączącej poszczególne kontrolery. Oznacza to nie tylko nowe możliwości rozbudowy systemu. Architektura sieci IP umożliwia użytkownikom tworzenie topologii z wieloma kontrolerami do obsługi większych terenów za pośrednictwem maksymalnie czterech zdecentralizowanych kontrolerów. W najszerszej konfiguracji system PAVIRO może obsługiwać do 984 stref, z sumaryczną mocą wzmacniaczy równą 164 000 W, dzięki czemu może być stosowany do tworzenia rozległych instalacji o dużej liczbie stref i głośników. Może być stosowany także w istniejących instalacjach, jeżeli infrastruktura budynku wymaga zmian i rozszerzenia systemu o kolejne pomieszczenia. Dodatkowo konfiguracja sieciowa stwarza możliwość utworzenia redundantnych kanałów, przez co poziom bezpieczeństwa obiektu wzrasta – w razie zagrożenia kanały te są zawsze dostępne i służą do emisji sygnałów ewakuacyjnych (także wtedy, gdy kontroler straci połączenie z siecią).

Bezpośr. inf.
Bosch Security Systems

Aplikacja mobilna
do zarządzania systemem kontroli dostępu RACS 5



Pakiet oprogramowania **VISO** przeznaczonego do zarządzania skalowanym systemem kontroli dostępu i automatyki budynkowej **RACS 5** firmy **ROGER** został powiększony o VISO Mobile. VISO Mobile jest aplikacją przeznaczoną do zdalnej obsługi systemu RACS 5 z poziomu urządzeń mobilnych z systemem Android. Aplikacja umożliwia zarządzanie uprawnieniami użytkowników systemu, w tym zarządzanie uprawnieniami gości. Możliwe jest również zdalne wydawanie komend, podgląd listy osób zalogowanych w danym obszarze systemu, ustalanie miejsca przebywania osób, monitorowanie zdarzeń w trybie online, a także przeglądanie zdarzeń zarejestrowanych w bazie danych systemu. Aplikacja jest przeznaczona dla użytkowników końcowych systemu RACS 5, którzy zajmują się bieżącą obsługą systemu, a w szczególności zarządzaniem uprawnieniami użytkowników oraz monitorowaniem ruchu osób. Mogą to być w szczególności pracownicy działu kadr lub ochrony budynku, który został objęty działaniem systemu.

Bezpośr. inf. ROGER

Ekspandery przejść do systemu RACS 5

Do zestawu urządzeń współpracujących z systemem **RACS 5** dodano nowe ekspandery we/wy typu **MCX2D** i **MCX4D**. Ekspandery są przeznaczone do kompleksowej obsługi czterech (MCX4D) lub dwóch (MCX2D) przejść zbudowanych na bazie czytników serii MCT z interfejsem komunikacyjnym RS485. Dla każdego z obsługiwanych przejść ekspandery udostępniają niezależną grupę zacisków zawierającą dwa wejścia, dwa wyjścia, dwa wyjścia zasilania (1,0 A i 0,2 A) oraz zaciski magistrali RS485. Wszystkie wyjścia ekspandera są zabezpieczone elektronicznie w taki sposób, by awaria na jednym przejściu nie miała wpływu na funkcjonowanie pozostałych przejść. Ekspandery wymagają zasilania z zewnętrznego zasilacza 13,8 V_{DC}, który jest jednocześnie źródłem zasilania kontrolera dostępu, czytników, zamków i innych elementów przejścia. Do każdego z obsługiwanych przejść ekspander dostarcza prąd 1,2 A, który z reguły wystarcza do zasilania elektrozaczepów rewersyjnych lub zwór magnetycznych. Ekspander współpracuje z akumulatorem rezerwowym, który, w zależności od potrzeb, może być ładowany prądem o wartości 0,3 A, 0,6 A lub 0,9 A. Dużym ułatwieniem w procesie podłączania przewodów elektrycznych i serwisowania ekspanderów są wyjmowane złącza śrubowe.

Pomimo tego, że ekspandery zostały zaprojektowane z myślą o obsłudze przejść, można je wykorzystać również do innych celów, tak jak standardowe ekspandery we/wy.

Ekspandery MCX4D i MCX2D są oferowane jako moduły elektroniczne lub w fabrycznych zestawach przeznaczonych do kontroli dostępu. Do zasilania ekspanderów rekomenduje się stosowanie zasilaczy sieciowych typu PS2D, PS4D i PS8D.

Bezpośr. inf. ROGER

Axis Partners' Day 2017
podsumowanie

13 września 2017 roku odbyła się kolejna edycja dorocznej konferencji **Axis Partners' Day**, podczas której eksperci z Axis Communications przedstawili najnowsze trendy i rozwiązania w branży sieciowych systemów dozorowych, w której firma jest liderem. W trakcie spotkania, które odbyło się w domu handlowym Vitkac w Warszawie, nagrodzono najlepszych uczestników Programu Partnerskiego Axis. Gościem specjalnym był Petr Tosner – dyrektor sprzedaży na Europę Wschodnią w firmie Axis Communications.

– Axis Partners' Day to dla nas ważna okazja do dialogu z naszymi partnerami, którzy stanowią wyjątkową grupę ekspertów na rynku zabezpieczeń. To miejsce wymiany doświadczeń, prezentacji najnowszych osiągnięć i najlepszych praktyk. Współpraca to klucz do sukcesu firmy Axis, a nasza sieć partnerów, resellerów i integratorów to atut, dzięki któremu byliśmy i wciąż jesteśmy liderami na rynku – powiedział Jakub Kozak, Sales Manager – Poland, Ukraine, Baltics.

Podczas spotkania wręczono nagrody dla członków Programu Partnerskiego Axis. W tym roku nagrodzono firmy mvb (Najlepszy Partner Roku 2017), ServiceLine (Debiut Roku 2017) oraz IB Systems (Najbardziej Dynamiczny Wzrost). Dodatkowo wyróżnienie za najciekawszy zrealizowany projekt przyznano firmie ELSTECH za implementację jednego z pierwszych w Polsce systemów kontroli dostępu firmy Axis Communications. Zaprezentowano także plany strategiczne firmy na najbliższy rok ze szczególnym uwzględnieniem współpracy w ramach dynamicznie rozwijanej sieci partnerskiej.

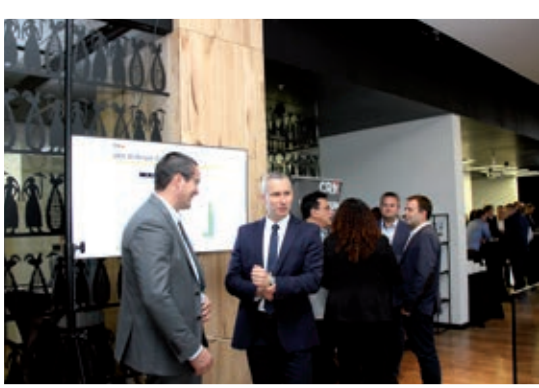
Podczas Axis Partners' Day 2017 omówiono, w jaki sposób szacować całościowy koszt systemu bezpieczeństwa z wykorzystaniem modelu całkowitego kosztu posiadania (ang. *Total Cost of Ownership* – TCO), który pozwala uwzględnić wszystkie koszty związane z systemem dozoru wizyjnego w całym okresie jego eksploatacji. Na spotkaniu obecny był Grzegorz Domagała, ekspert w zakresie doskonalenia procesów sprzedaży B2B, który przedstawił zasady działania według metody CustomerCentric Selling. Dużo uwagi poświęcono kwestii cyberbezpieczeństwa urządzeń i systemów do monitorowania – kluczowego z powodu rosnącego zagrożenia ze strony cyberprzestępców.

Zgromadzeni goście mieli okazję zapoznać się z najciekawszymi nowościami z oferty firmy Axis Communications, takimi jak kamery wykorzystujące technikę radarową, a także z zapowiedziami zbliżających się premier rynkowych. Eksperci zaprezentowali także koncepcję kompleksowych rozwiązań dla poszczególnych segmentów rynku, które umożliwią najlepsze wykorzystanie parametrów i możliwości urządzeń Axis.

Więcej informacji o firmie Axis Communications można znaleźć na stronie internetowej pod adresem www.axis.com.

Bezpośr. inf.
Axis Communications

Zapraszamy do obejrzenia fotorelacji na stronie http://www.zabezpieczenia.com.pl/fotogalerie.



Jubileuszowe XXV Ogólnopolskie Warsztaty SAP 2017

podsumowanie

Janów Podlaski jest znany na całym świecie ze stadniny koni arabskich, ale dla specjalistów z branży zabezpieczeń najważniejsze są odbywające się tam **warsztaty SAP**.

Pierwsze działania przygotowawcze rozpoczęły się jeszcze w październiku ubiegłego roku. Najpierw były intensywne poszukiwania wyjątkowego miejsca, które spełniłoby wszystkie nasze wymagania. Udało się! Wybraliśmy piękny, odbudowany z ruin Zamek Biskupi z interesująco zagospodarowanym podzamczem, wyśmienitą kuchnią i profesjonalną obsługą.

Nadszedł wrzesień. Zdążyliśmy zaprezentować nasze urządzenia podczas Międzynarodowych Targów FIREX 2017 w Londynie, a potem, od 4 do 7 września, uczestniczyliśmy w Międzynarodowym Salonie Przemysłu Obronnego MSPO 2017 w Kielcach – w największej tego typu imprezie w Europie. Choć byliśmy uczestnikiem tych targów po raz pierwszy, były dla nas owocne i bardzo udane.

Minął tydzień i trzeba było przenieść się do Janowa Podlaskiego. Specjalnie podkreślam słowo „Podlaski" ponieważ niektórzy klienci szukali naszej imprezy w Janowie, ale Lubelskim. W związku z tym, że przyznali się nam do tej pomyłki, piszę o tym z uśmiechem.

25 LAT WARSZTATÓW SAP

POLON-ALFA

Punktualnie o godzinie 15. w środę 20 września, zwarci i gotowi, oczekiwaliśmy na pierwszych gości. Recepcja hotelowa szybko zaczęła zapełniać się uczestnikami **XXV Ogólnopolskich Warsztatów SAP 2017**. Nawet się nie obejrzeliśmy, a już lista obecności zapełniła się podpisami. Pierwszy wieczór upłynął na rozmowach w zamkowych pokojach i na podzamczu.

Oficjalne uroczyste otwarcie jubileuszowych warsztatów poprzedził film przygotowany specjalnie na tę okazję. Wywoływał on wzruszenie, ale momentami również gromki śmiech. Wśród gości zgromadzonych na sali znalazł się jeden wyjątkowy – p. Zbigniew Slanina z firmy SUPOL Będzin. To jedyny uczestnik wszystkich dwudziestu pięciu edycji warsztatów. Z tego powodu prezes firmy Polon-Alfa – Dariusz Nagański – uhonorował tego wyjątkowego uczestnika statuetką przygotowaną specjalnie na tę okazję.

Po pierwszym miłym akcencie nastąpiły kolejne. Bronisław Skaźnik i Krzysztof Dąbrowski – prezes i sekretarz generalny Stowarzyszenia Inżynierów i Techników Pożarnictwa, a także przedstawiciele Klubu Generalskiego Państwowej Straży Pożarnej – generał brygadier w st. spoczynku Wiesław Leśniakiewicz oraz nadbrygadier w st. spoczynku Roman Kaźmierczak, złożyli serdeczne gratulacje z okazji jubileuszu i przekazali na ręce prezesa Nagańskiego okolicznościowe listy.

Merytoryczną część warsztatów SAP 2017 rozpoczął wykład Waldemara Wnęka ze Szkoły Głównej Służby Pożarniczej pt. *Sterowanie urządzeniami gaśniczymi*. W bardzo przystępny sposób przedstawił on wszystkie zalecenia i wymagania dotyczące działania systemów gaszenia. Wykład został uzupełniony bardzo ciekawymi przykładami i zdjęciami.

Kolejny wykład wygłosiła Daria Kubis – przedstawicielka CNBOP – PIB. Przybliżyła ona całe spektrum technicznych możliwości stałych urządzeń gaśniczych. Przedstawiła wszystkie obecnie dostępne techniki gaszenia wraz z ich zaletami i wadami. Obecni na sali projektanci szczególnie uważnie wsłuchiwali się, gdy omawiane były wady, ponieważ to właśnie oni muszą pamiętać, że odpowiednio dobrane medium gaszące nie może być zagrożeniem dla mienia w strefie objętej systemem gaszenia.

Następny wykład wygłosił Przemysław Kubica – przedstawiciel Szkoły Głównej Służby Pożarniczej. Jego wystąpienie stanowiło swoistą kontynuację wykładów przedmówców. Omówił on projektowanie gazowych instalacji automatycznego gaszenia i zalecenia dotyczące wykonawstwa i konserwacji.

Wieczorem odbył się koncert wyjątkowego kwartetu smyczkowego – Grupy MoCarta. Nie zabrakło również jubileuszowego tortu, którego pierwszy kawałek odkroił prezes firmy Polon-Alfa. W fantastycznej atmosferze odbyła się kolacja, a wykwintne dania i żywiołowe rozmowy sprawiły, że ostatnich uczestników żegnały pierwsze promienie wschodzącego słońca.

Zbigniew Slanina, Supol, uczestnik wszystkich 25 edycji warsztatów

„To bardzo przyjemne spotkania. Jest grupa ludzi, z którymi spotykamy się od wielu, wielu lat (...). Impreza jest nie tylko miła, ale też bardzo dokształcająca. Za każdym razem wynosi się z tych warsztatów coś nowego (...). Na pewno ci, którzy chcieli, mogli skorzystać, a poza tym można było dyskutować na wiele tematów. Jak zdrowie pozwoli, spotkamy się znowu za rok!"

Waldemar Wnęk, Szkoła Główna Służby Pożarniczej, uczestnik wielu edycji warsztatów

„Żeby nie Polon, to pewnikiem tylu wytycznych by nie było (wytycznych dotyczących projektowania – przyp. red.). Trzeba przyznać, że firma Polon-Alfa bardzo dużo zrobiła dla ułatwiania procesu projektowego, już nie mówiąc o tym, że w wytyczne SITP-u bardzo duży wkład mieli właśnie pracownicy firmy Polon-Alfa. Życzę dalszego nieustającego rozwoju firmy i warsztatów!"

Drugi dzień warsztatów rozpoczął się wykładem Doroty Brzezińskiej z Politechniki Łódzkiej pt. *Strategiczne myślenie jako nowa metoda oceny bezpieczeństwa pożarowego budynków*. Wykład ten przybliżył słuchaczom analityczne podejście do przeciwpożarowego zabezpieczania obiektów.

Następnie Edward Skiepko z SGSP wygłosił wykład pt. *Funkcjonowanie instalacji sterujących gaszeniem w warunkach pożaru*. Wykładowca ma dużą wiedzę teoretyczną, ale przede wszystkim jest praktykiem, który przykłada wagę do zagadnień związanych z zasilaniem systemów bezpieczeństwa. Trzeba przyznać, że jego spojrzenie na problematykę zasilania rzuca nowe światło na to zagadnienie, a więc również na jakość pracy całego zabezpieczenia pożarowego w obiekcie.

Daria Kubis, CNBOP-PIB, pierwszy raz na warsztatach

„Organizacja oraz liczba uczestników robi wrażenie. Jadąc do Państwa, nie spodziewałam się, że będzie aż tyle zainteresowanych osób. Bardzo się cieszę, że mogę tu być i dziękuję za zaproszenie"

Kolejny wykład wygłosił Mariusz Sobecki – rzeczoznawca ds. zabezpieczeń przeciwpożarowych. To osoba, która od wielu lat

bierze udział w naszych warsztatach, zarówno jako uczestnik, jak i wykładowca. Wystąpienie na temat odbiorów i eksploatacji systemów sterowania gaszeniem było naprawdę dobrą lekcją dla wszystkich słuchaczy. Wykładowca przypomniał, na co należy zwracać uwagę, a także omówił możliwe nieprawidłowości w instalacjach. Odwoływał się do przepisów, więc słuchacze uzyskali szczególnie potrzebne w zawodowej działalności informacje.

Florin Jacobine, Astal Rumunia, pierwszy raz na warsztatach

„Jest bardzo miło (...). Organizacja warsztatów jest bardzo dobra. Jest to najlepsza impreza branżowa, na jakiej byłem, od wielu lat. Gratulacje!"

Ostatni z wykładów w ramach merytorycznej części warsztatów SAP 2017 wygłosił Robert Kuczkowski z PZU Lab. Już drugi raz przedstawiciel tej instytucji wziął udział w naszych warsztatach jako wykładowca. Robert Kuczkowski omówił problem możliwych strat spowodowanych nieprawidłowym doborem lub nieprawidłowym działaniem instalacji gaśniczych. Słuchacze po raz kolejny przekonali się, że najczęściej uczymy się na błędach. Dowiedziawszy się, co jest błędem, można go uniknąć, aby lepiej wykorzystać dostępne środki techniczne.

Jubileuszowe warsztaty SAP 2017 zostały wysoko ocenione przez wszystkich uczestników. Uczestnikom przekazali wiedzę najlepsi specjaliści z branży.

Piątkowy wieczór upłynął przy dźwiękach przebojów świętującego swoje 30-lecie zespołu De Mono. Dzięki charyzmie wokalisty Andrzeja Krzywego, fantastycznym piosenkom i profesjonalizmowi muzyków zespół porwał na parkiet większość uczestników.

Tradycyjnie na warsztatach zorganizowano wystawę urządzeń z oferty firmy Polon-Alfa. Tym razem jednak, ku zaskoczeniu gości, wystawiony sprzęt był podzielony na dwie części. W pierwszej części znalazł się system sygnalizacji pożarowej POLON 6000. To największa duma firmy, system dobrze przyjęty przez użytkowników. Nasi goście zasypywali nas pytaniami o kierunek dalszego rozwoju tego wyjątkowego systemu. Podczas prezentacji nowych rozwiązań z oferty firmy Polon-Alfa przedstawione zostały niedawno wprowadzone w systemie funkcje, dlatego zainteresowanie było ogromne.

Józef Kuchar, ROP INSTAL Józef Kuchar, pierwszy raz na warsztatach

„Wysoki poziom warsztatów, wspaniała organizacja – tak, że tylko pochwalić. (...) gratuluję fantastycznej imprezy"

Centralną część ekspozycji stanowiły nowe urządzenia z oferty firmy Polon-Alfa. Dwie nowości zostały omówione w ramach prezentacji. Pierwsza z nich to właśnie opracowany i poddawany badaniom system sterowania gaszeniem z nową centralą IGNIS 2500. Centrala ta jest wyrazem nowego podejścia do realizacji sterowania gaszeniem. Modułowa konstrukcja, w której zastosowano sprawdzone rozwiązania znane z central UCS 6000 i POLON 6000, to duży postęp, a możliwość łączenia central ze sobą pozwoli optymalnie dostosować sprzęt do potrzeb odbiorcy. Propozycja ta spotkała się z entuzjastycznym przyjęciem i wielkim zainteresowaniem, które było dodatkowo wzmagane przez możliwość pracy adresowalnej w komunikacji z centralą POLON 6000.

Drugi system, który został przedstawiony jako nowość, to system detekcji gazów SDG 6000, który właśnie został wprowadzony do sprzedaży. Wzbudził on tak samo duże zainteresowanie.

Na końcu zaprezentowano centralę UCS 6000. To urządzenie jest unikatem wśród urządzeń bezpieczeństwa pożarowego i od paru lat cieszy się niesłabnącym popytem.

Warto podkreślić to, co najistotniejsze i jednocześnie niespotykane u jakiegokolwiek innego producenta systemów bezpieczeństwa pożarowego na świecie – informacje ze wszystkich opisanych powyżej urządzeń mogą być odczytane w jednym systemie nadrzędnym, którym jest POLON 6000. Dzięki wspólnemu protokołowi komunikacyjnemu obsługa może odebrać w nim sygnały z różnych, powiązanych ze sobą systemów i zareagować na nie.

Oprócz nowych produktów przedstawione zostały urządzenia, których produkcja została zakończona, w niektórych przypadkach wiele lat temu. Wśród zaprezentowanych urządzeń były centrale TELSAP T3, CSP-35, ALFA-3800 i wiele czujek. To swoiste muzeum systemów

Czesław Podstawny, CAMAR, 24 razy na warsztatach

„Jestem zaskoczony liczbą uczestników. To chyba są największe warsztaty, na jakich byłem. Bardzo dużo ludzi, no i – co widać – dużo młodych, czyli branża się rozwija"

Marcin Slanina, Supol, pierwszy raz na warsztatach

„Formuła warsztatów jest mi dobrze znana, ponieważ, odkąd pamiętam, ojciec przekazywał mi wszystko za każdym razem, kiedy z nich wracał. Zawsze było to wydarzenie bardzo interesujące. Mam nadzieję, że będę mógł uczestniczyć w kolejnych edycjach – przynajmniej przez 25 lat...”

sygnalizacji pożarowej wywoływało nostalgię i przyciągnęło wielu oglądających. Wspomnieniom towarzyszyły silne emocje, bo przecież urządzenia te przypominały o wielu dobrych chwilach. Niektórych dotyczą anegdoty i historie, np. o tym, ile

Elżbieta Szczepańska, Atomsystem, uczestniczka pierwszej edycji, dwudziesty raz na warsztatach

„Z nostalgią wspominam Zacisze, czyli miejsce, w którym wszystko się zaczęło. Chyba nikt nie przewidywał, że zaczynamy coś tak wyjątkowego. Spotkanie o wysokim poziomie merytorycznym stworzyło możliwość integracji środowiska. To był strzał w dziesiątkę”

czasu trwała podróż do siedziby firmy Polon-Alfa w celu odbioru sprzętu. Te ciekawe historie opowiadali nasi goście. Wspominali też pierwsze edycje warsztatów, brak zasięgu telefonii komórkowej, błądzenie po pozbawionej drogowskazów drodze w Borach Tucholskich, rejsy Niwą i kawę po kapitańsku, ujeżdżanie byka, walki gladiatorów i dojenie krowy, ale przede wszystkim wspaniałą atmosferę i specyficzny klimat, który od początku towarzyszył tej imprezie.

Jubileuszowe XXV Ogólnopolskie Warsztaty SAP 2017 przeszły do historii. Jeszcze pewnie nie raz będziemy wracać do zdjęć i wspomnień z tej wyjątkowej imprezy. Dziękujemy wszystkim gościom, wykładowcom i uczestnikom za to, że postanowili z nami świętować ten jubileusz. Dziękujemy za wszystkie ciepłe słowa, gratulacje, wspomnienia i anegdoty, które z pewnością na długo zostaną w pamięci, a także zmobilizują nas do dalszego działania.

Janos Manyi, Astal Węgry, pierwszy raz na warsztatach

„Bardzo udana konferencja, ogromna liczba uczestników, bardzo ciekawe miejsce. Widać, że branża systemów sygnalizacji pożarowej w Polsce jest na bardzo wysokim poziomie, a uczestnicy chętnie zdobywają nową wiedzę. Chciałbym zorganizować podobne warsztaty na Węgrzech”

Już dzisiaj serdecznie zapraszamy na kolejną edycję tej imprezy, która odbędzie się w dniach **19–22 września 2018 r.** Do zobaczenia!

Bezpośr. inf. Elżbieta Czajka
Polon-Alfa

Międzynarodowa konferencja

Ochrona dóbr kultury na wypadek szczególnych zagrożeń – wybrane aspekty ewakuacji osób i zbiorów – podsumowanie

W dniach 20–22 września 2017 r. w Krakowie odbyła się międzynarodowa konferencja *Ochrona dóbr kultury na wypadek szczególnych zagrożeń – wybrane aspekty ewakuacji osób i zbiorów*. Zorganizowała ją Szkoła Aspirantów Państwowej Straży Pożarnej przy współudziale Szefa Obrony Cywilnej Kraju-Komendanta Głównego Państwowej Straży Pożarnej, we współpracy z Ministerstwem Kultury i Dziedzictwa Narodowego, Międzynarodowym Centrum Kultury w Krakowie, Polskim Komitetem Błękitnej Tarczy oraz Komendą Wojewódzką PSP w Krakowie. Konferencja ta jest organizowana cyklicznie co dwa lata od początku lat dziewięćdziesiątych dwudziestego wieku. Honorowy patronat objęli:

– prof. dr hab. Piotr Gliński – wiceprezes Rady Ministrów, Minister Kultury i Dziedzictwa Narodowego,
– Sławomir Frątczak – dyrektor Departamentu Edukacji, Kultury i Dziedzictwa MON,
– generał brygadier Leszek Suski – komendant główny Państwowej Straży Pożarnej i szef Obrony Cywilnej Kraju,
– nadbrygadier Stanisław Nowak – małopolski komendant wojewódzki PSP,
– Jacek Krupa – marszałek województwa małopolskiego,
– Jacek Majchrowski – prezydent Krakowa,
– Polski Komitet ds. UNESCO,
– Prezes Polskiego Komitetu Błękitnej Tarczy,
– Narodowy Instytut Muzealnictwa i Ochrony Zbiorów,
– Narodowy Instytut Dziedzictwa.

W tym roku wśród 147 uczestników konferencji byli między innymi właściciele i zarządcy obiektów zabytkowych, pracownicy muzeów, bibliotekarze, archiwiści, przedstawiciele urzędów i instytucji zainteresowanych ochroną dóbr kultury, przedstawiciele Państwowej Straży Pożarnej, Wojska Polskiego, policji i Straży Miejskiej, służb ochrony, komórek zajmujących się zarządzaniem kryzysowym, służb ratowniczych, administracji rządowej i samorządowej. W konferencji uczestniczył także małopolski wojewódzki konserwator zabytków – dr inż. arch. Jan Janczykowski.

Pierwsza sesja odbyła się 20 września w siedzibie Międzynarodowego Centrum Kultury mieszczącej się na Rynku Głównym w Krakowie. Uczestników konferencji powitali zastępca dyrektora MCK Piotr Bąk, komendant Szkoły Aspirantów PSP w Krakowie kpt. Marek Chwała oraz małopolski komendant wojewódzki PSP w Krakowie nadbryg. Stanisław Nowak. Został także odczytany list, który do uczestników konferencji skierowała dr hab. prof. IH PAN Magdalena Gawin – wiceminister kultury i dziedzictwa narodowego, generalny konserwator zabytków.


301 25
KR 489HS

Podczas pierwszej sesji wygłoszono referaty dotyczące międzynarodowego prawa humanitarnego, zagrożeń i ochrony zabytków, dwudziestu lat działalności Centrum Szkolenia Ochrony Ludności i Dóbr Kultury, programu Błękitnej Tarczy oraz praktycznych rozwiązań z zakresu zabezpieczenia zabytkowych obiektów i stosowanych w tym celu rozwiązań technicznych i organizacyjnych. W ramach tej sesji Leszek Mazan przedstawił także historię Krakowa i mówił na temat pożarów, które miały miejsce w Krakowie w przeszłości.

Druga sesja, która odbyła się 21września, miała miejsce w auli Szkoły Aspirantów PSP w Krakowie. Tematyka sesji obejmowała historię i współczesność Bazyliki Mariackiej w Krakowie, problemy związane z działaniem służb ratowniczych w gęsto zabudowanych zabytkowych centrach miast, wpływ różnorodnych barier architektonicznych na efektywność działań ratowniczych oraz założenia dotyczące ćwiczeń w Bazylice Mariackiej. Omówiono także utrudnienia związane z organizowaniem i odbywaniem się praktycznych ćwiczeń w zabytkowym obiekcie, w którym mogą przebywać duże grupy turystów i wiernych (także obcojęzyczne) i który znajduje się w ścisłym centrum miasta.

W tym samym dniu, w ramach trzeciej sesji, odbyły się ćwiczenia z ewakuacji osób i zbiorów z Bazyliki Mariackiej w Krakowie. Scenariusz ćwiczeń – ze względu na chęć zachowania jak najbardziej rzeczywistych warunków – nie przewidywał przerwania ruchu turystycznego, dzięki czemu uczestnicy konferencji byli świadkami ogłoszenia ewakuacji (w kilku językach) przez dźwiękowy system ostrzegawczy, ewakuacji turystów i działań prowadzonych przez pracowników bazyliki odpowiedzialnych za ewakuację turystów i modlących się. Mogli też oglądać na telebimie bezpośrednią transmisję obrazu z wnętrza Bazyliki. Wszystko odbywało się w czasie rzeczywistym, więc biorące udział w ćwiczeniach zastępy z Komendy Miejskiej PSP oraz ze Szkoły Aspirantów PSP w Krakowie uwzględniły odległość

od miejsca zdarzenia i panujące warunki drogowe. Zastępy te wykonywały zadania mające na celu ugaszenie pożaru, zabezpieczenie miejsca zdarzenia oraz ewakuację osób i zbiorów. Kolejność ewakuacji obiektów zabytkowych, miejsce, w które były przenoszone, a także sposób zabezpieczenia był na bieżąco uzgadniany z przedstawicielami zarządzającego Bazyliką Mariacką. Kolejnym elementem ćwiczeń była ewakuacja hejnalisty oraz gaszenie pożaru poddasza.

Tego samego dnia, dzięki zaproszeniu dyrektora Muzeum Narodowego w Krakowie, uczestnicy konferencji mieli okazję obejrzeć wystawę ***#dziedzictwo***, po której oprowadzał ich jej twórca i kurator – wicedyrektor Muzeum Narodowego w Krakowie dr hab. Jan Szczerski.

Czwarta sesja odbyła się 22 września w auli Szkoły Aspirantów PSP w Krakowie. Wygłoszono referaty dotyczące zagrożeń i sposobów ewakuacji obiektów zabytkowych i osób, współpracy konserwatorów dzieł sztuki ze służbami ratowniczymi i zakresu działalności konserwatorów, a także omówiono dwa przykłady działań ratowniczych oraz współpracy zarządców ze służbami ratowniczymi – działań podjętych w związku z katastrofą budowlaną w Zamku Książąt Pomorskich w Szczecinie oraz pożarem katedry w Gorzowie Wielkopolskim. Omówiono również aspekty organizacji ćwiczeń w obiektach zabytkowych.

Na zakończenie konferencji przyjęto jednogłośnie komunikat końcowy, w opracowaniu którego uczestniczyli także członkowie działającej przy Komendancie Głównym PSP rady programowej ds. ochrony dóbr kultury przed nadzwyczajnymi zagrożeniami.

Kolejna konferencja z tego cyklu planowana jest na **wrzesień 2019 roku.**

Bezpośr. inf.
bryg. Krzysztof Kociołek
Szkoła Aspirantów PSP

Jubileuszowe Spotkanie Projektantów Instalacji Niskoprądowych

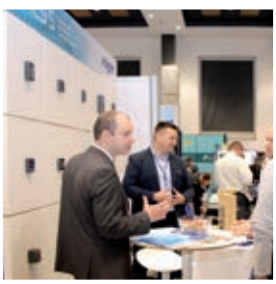
podsumowanie

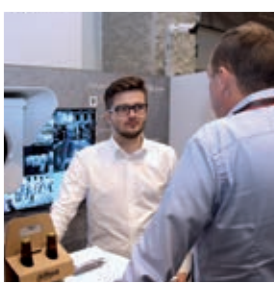
W dniach **27–28 września 2017** w Nosalowym Dworze **w Zakopanem** odbyło się piętnaste Spotkanie Projektantów Instalacji Niskoprądowych (**SPIN**). Organizatorem była firma **Lockus**. Wyjątkowa, jubileuszowa edycja zgromadziła ponad 320 uczestników.

Nowością była strefa stoisk wystawienniczych, a także indeksy, które spotkały się z entuzjastycznym przyjęciem partnerów i gości. Ich celem było zachęcanie uczestników do odwiedzania stoisk partnerów.

Nie zabrakło atrakcji, które miały na celu integrację uczestników SPIN-u i uczczenie jubileuszu w wyjątkowy sposób. Były też zajęcia na zewnątrz oraz uroczysta kolacja połączona z występami artystycznymi.

Prezentacja ekspercka podczas jubileuszowej edycji SPIN-u została dokonana pod patronatem merytorycznym Polskiej Izby Systemów Alarmowych (PISA). Prelekcję na temat techniki termowizyjnej i wykorzystania dronów w branży zabezpieczeń wygłosił Jakub Sobek.





Wśród partnerów tegorocznej, południowej edycji znaleźli się:
– Złoci Partnerzy: AAT Holding S.A., BKT Elektronik, Dahua Technology, Hikvision, Pulsar, QNAP z Western Digital;
– Srebrni Partnerzy: ABB, Ambient System, ASSMANN, BCS, Corning Optical Communications, DTS SYSTEM z firmą Bosch, European Security Trading EST, Grupa ROMI, Hanwha Techwin, Impakt z produktami marki Power Walker, Milestone, Nedap, Polon Alfa, RCS Engineering wspólnie z UAVS Polska, ROGER, SALTO Systems, TP-Link, Zettler;
– Brązowi Partnerzy: CIAS, Datwyler, DRX Group, Extreme Networks z Veracomp, GEO Kat, Micro-Made, MKJ, Raban Sp. j. T. Żmójdzin.

Zapraszamy do obejrzenia zdjęć (https://www.flickr.com/gp/105872726@N08/c8B9Ee).

Bezpośr. inf. Lockus

Zapraszamy do obejrzenia fotorelacji na stronie http://www.zabezpieczenia.com.pl/fotogalerie.

Zdalny nadzór wizyjny
sposobem na obniżenie kosztów ochrony

Daniel Kamiński

W Europie Zachodniej koszt utrzymania pracownika ochrony dochodzi nawet do 15 EUR za godzinę i jest wyższy niż koszt stosowania autonomicznych robotów wyposażonych w kamery (!). W Polsce koszt utrzymania pracownika ochrony do niedawna wynosił nie więcej niż 1 EUR, dlatego mieliśmy najwięcej pracowników ochrony w Europie

Przez ostatnie 25 lat zabezpieczenia techniczne rozwijały się w Polsce zdecydowanie wolniej niż w krajach Europy Zachodniej. Świetnie natomiast rozwijały się usługi ochrony fizycznej, co doprowadziło do nie spotykanych w innych europejskich krajach anomalii – liczba pracowników ochrony fizycznej była większa niż liczba funkcjonariuszy policji i wojska razem. Przyczyną tej sytuacji były niskie wynagrodzenia minimalne – postawienie wartownika było tańsze niż skorzystanie z technicznych systemów zabezpieczeń.

Zeszłoroczny wzrost wynagrodzeń minimalnych spowodował wzrost wynagrodzeń dla ochroniarzy, dlatego firmy zajmujące się ochroną fizyczną musiały renegocjować ceny ze swoimi klientami. Niestety większość inwestorów nie była przygotowana na wyższe ceny. W związku z tym liczba pracowników ochraniających obiekty została zredukowana i próbowano wymyślać, jak utrzymać bezpieczeństwo na odpowiednim poziomie przy zredukowanym personelu.

W efekcie zmian wypracowany został nowy model ochrony –wyposażono chronione obiekty w kamery i przeniesiono część pracowników do zdalnych centrów nadzoru wizyjnego. Niestety z powodu braku wypracowanych standardów zapanowała zupełna dowolność w świadczeniu usług zdalnego nadzoru wizyjnego. Firmy pobierają podobne opłaty, jednak oferują różne usługi, nazywając je tak samo – nadzorem wizyjnym. Część z nich oferuje przeniesienie stałego nadzoru wizyjnego, który był realizowany bezpośrednio w obiekcie, część wizyjną weryfikację przyczyn alarmów, a część okresową kontrolę z wykorzystaniem kamer (patrole wizyjne).

Rodzaje usług zdalnego nadzoru wizyjnego

Usługa zdalnego nadzoru wizyjnego powstała w celu zoptymalizowania kosztu usług związanych z ochroną. Głównym założeniem takiego rozwiązania jest instalacja kamer w chronionym obiekcie i przeniesienie pracownika ochrony z obiektu do zdalnego centrum monitorowania. Żeby obniżyć koszty, pracownik musi obsługiwać kamery znajdujące się w kilku czy nawet kilkunastu obiektach.

Zdalny nadzór wizyjny może być realizowany na kilka sposobów. Najczęściej operatorzy przebywający w centrum monitorowania obserwują chroniony obiekt za pomocą kamer. Jest to najdroższy sposób. Tak naprawdę operator ma ograniczoną percepcję, więc może obsługiwać kamery z maksymalnie dwóch obiektów, czyli obserwować ok. 32 obrazów. Aby obniżyć koszty usługi, bardzo często konieczne jest zwiększenie liczby obsługiwanych kamer, co osiąga się, obserwując na zmianę obrazy z kamer znajdujących się w różnych obiektach. W ten sposób operator może obsługiwać cztery razy więcej obiektów, czyli nawet 120 kamer. Dzięki takiemu podejściu usługa może być oferowana za 200 zł od kamery miesięcznie, co powoduje, że zdalna ochrona obiektu kosztuje cztery razy mniej niż pojedynczy posterunek.

Okresowe patrole wizyjne są kolejnym sposobem na obniżenie kosztów ochrony. Usługa polega na okresowym łączeniu się z chronionym obiektem i wzrokowym sprawdzeniu za pomocą kamer, jaka sytuacja w nim panuje. W usłudze przeznacza się ok. 20–30 sekund na obserwację obrazu z jednej kamery, co pozwala obsłużyć ok. pięciu obiektów w ciągu godziny. Przy założeniu, że operator wykonuje patrol wizyjny cztery razy na dobę, może on obsłużyć 30 obiektów, co oznacza obserwację obrazów z aż 480 kamer. W przypadku takiej usługi cena może być na poziomie 50 zł od każdej z kamer. W porównaniu z kosztem posterunku cena patroli wizyjnych jest bardzo atrakcyjna. Wymaga jednak zaakceptowania tego, że operator łączy się z obiektem co kilka godzin i obserwuje obrazy z kamer przez około 10 minut. Do tej ceny należy dodać opłatę za gotowość oraz za reakcję grup interwencyjnych.

Najtańsza jest wizyjna weryfikacja przyczyn alarmów. W przypadku tej usługi połączenie z obiektem następuje tylko wówczas, gdy lokalny system alarmowy lub program dokonujący analizy treści obrazu wywoła alarm. Operator obserwuje bieżące obrazy z kamer oraz sprawdza tzw. prealarm w celu ustalenia, jakie zdarzenie doprowadziło do wygenerowania alarmu. Obsługa zajmuje trochę więcej czasu niż patrol wizyjny, ale alarmy są generowane przez kamery co najwyżej kilka razy w miesiącu, więc usługa kosztuje ok. 20 zł od kamery.

Optymalnym ze względu na koszt rozwiązaniem jest łączenie weryfikacji wizyjnej z patrolami wizyjnymi. Uzyskuje się dzięki niemu reakcję na alarm oraz uruchamia prewencyjne połączenia mające na celu wykrycie anomalii. Z reguły koszt łącznej oferty nie przekracza 100 zł od kamery. Niestety tego typu usługę mogą zaoferować tylko firmy posiadające oprogramowanie przygotowane od obsługi zdarzeń zauważanych przez kamery. Ze względu na złożoność usług nie uda się prowadzić tego typu dozoru wizyjnego, bazując na darmowych programach VMS. Ponadto z powodu różnorodności rozwiązań stosowanych w centrach monitorowania firmy zajmujące się ochroną musiałyby mieć osobne stanowiska z różnymi programami VMS dostosowanymi do urządzeń różnych producentów, co jest bardzo trudne do zrealizowania.

Stosowane rozwiązania techniczne

Każda z opisanych usług łączy się ze specyficznymi wymaganiami dotyczącymi sprzętu, na którym będzie realizowana. W przypadku zdalnego nadzoru wizyjnego wykorzystywane są standardowe funkcje zdalnego dostępu do rejestratorów i kamer IP. Jeden ze strumieni wizyjnych o niskiej jakości (4CIF/D1) jest przesyłany do centrum nadzoru wizyjnego. Taka jakość wystarczy, by operator zainterweniował. W przypadku wątpliwości operator może sprawdzić archiwum z nagraniami o jakości FullHD. Odczyt obrazów o takiej jakości jest jednak wyzwaniem z powodu dostępności pasma sieciowego zarówno w chronionym obiekcie, jak i w centrum monitorowania.

Wyzwaniem dla firm zajmujących się ochroną jest też integracja urządzeń różnych producentów. Z tego względu stosuje się rozwiązania maksymalnie 2–3 producentów. Korzystanie ze zbyt wielu zaawansowanych funkcji jest trudne.

Liczba wysoko wykwalifikowanych pracowników technicznych jest ograniczona. Lata dominacji ochrony fizycznej doprowadziły do tego, że wiele firm zajmujących się ochroną zrezygnowało z własnych działów technicznych i działów IT. Dodatkowym utrudnieniem był i jest niedobór takich specjalistów jak informatycy ze względu na mały prestiż branży ochrony – wybierają oni inne branże.

Częściowym rozwiązaniem problemów firm zajmujących się ochroną jest zastosowanie uniwersalnych transmiterów strumieni wizyjnych. Umożliwiają one połączenie z dowolnym systemem wizyjnym zainstalowanym u klienta, ograniczenie ilości niezbędnych zasobów oraz uproszczenie szkolenia nowych pracowników. Transmitery wizyjne umożliwiają integrację sprzętową, co jest bardzo wygodne dla służb technicznych, oraz korzystanie z jednego oprogramowania, co jest bardzo przydatne dla operatorów centrum monitorowania.

Współczesne transmitery wizyjne mają bogatą historię poza granicami Polski. W innych krajach są stosowane od kilkudziesięciu lat, dlatego są przygotowane do pracy zarówno na łączach telefonicznych, jak i internetowych. Jedną z ich największych zalet jest możliwość korzystania z funkcji analizujących treść obrazu, które przyczyniają się do ułatwienia detekcji intruzów. Transmitery umożliwiają podłączenie zewnętrznych czujek ruchu oraz głośników i w efekcie realizację procedur weryfikacji przyczyn alarmów oraz podjęcie natychmiastowej interwencji głosowej.

Oprogramowanie wspomagające nadzór wizyjny

Realizacja usług zdalnego nadzoru wizyjnego jest praktycznie niemożliwa bez specjalistycznego

oprogramowania, przy czym trzeba zaznaczyć, że programy typu VMS lub PSIM (Physical Security Information Management), które sprawdzają się w centrach monitorowania BMS, nie mają zastosowania w centrach zdalnego nadzoru wizyjnego prowadzonych przez firmy zajmujące się ochroną. Z tego względu firmy tworzące programy do obsługi alarmów musiały dopisać moduły do obsługi zdarzeń wykrywanych metodami wizyjnymi.

Z tego powodu za pomocą programów dostępnych na polskim rynku można realizować jedynie usługi opisane powyżej. Dostępne są moduły służące do zdalnego nadzoru wizyjnego. Przypominają one ściany monitorów z programów VMS, ale mają więcej funkcji. Umożliwiają dopisywanie komentarzy operatorów do historii zdarzeń alarmowych. Obsługa zdarzeń jest powiązana z procedurami zależnymi od pory dnia oraz innymi procedurami realizowanymi zgodnie z wprowadzonymi harmonogramami. Do tego dołączane są dane kontaktowe osób, które należy powiadomić w przypadku zdarzenia.

Kolejną funkcją niespotykaną w programach typu VMS jest obsługa wirtualnych patroli wizyjnych. Główny nacisk jest kładziony na właściwe zdefiniowanie obrazów referencyjnych i przypisanie im procedur do wykonania w trakcie połączenia. Może to być sprawdzenie, czy drogi sprzęt jest na swoim miejscu w warsztacie albo czy drzwi na zaplecze w sklepie są zamknięte. Główną zaletą jest to, że operator w czasie patrolu widzi, jak powinna wyglądać scena, i porównuje ten wzorcowy obraz z obrazem z kamery. Ma również podgląd prealarmu bez potrzeby przeglądania materiału archiwalnego, więc może od razu podjąć decyzję dotyczącą sytuacji w obiekcie. W przypadku obiektów nadzorowanych tylko w nocy programy umożliwiają wykonanie dodatkowego zdjęcia referencyjnego w momencie przejmowania służby.

Programy do obsługi alarmów mają jeszcze jedną właściwość, a mianowicie pozwalają traktować rejestrator, kamerę IP lub nadajnik wizyjny jako element systemu alarmowego, więc pobudzenie wejść alarmowych tych urządzeń lub wewnętrzne usterki będą traktowane jako wydarzenia wymagające obsługi. Zanik sygnału wizyjnego z kamery, detekcja intruza czy awaria dysku to zdarzenia, na które operator zareaguje i które zostaną odnotowane w dzienniku zdarzeń. Najbardziej istotne jest jednak to, że operatorzy mają jeden program do obsługi systemów alarmowych i systemów wizyjnych, więc mogą sprawnie podejmować decyzje.

Należy stanowczo stwierdzić, że usługi dozoru wizyjnego są tak skuteczne jak zastosowane w nich procedury, które zostaną uzgodnione z klientem. Tu pojawia się kolejny problem. Olbrzymia oferta sprzętowa, różnorodność funkcji oraz brak wypracowanych standardów powoduje, że procedury nie są uzgadniane. Trzeba podkreślić, że część firm zajmujących się ochroną uruchomiła usługi zdalnego nadzoru wizyjnego bez uzgodnienia procedur z klientami. W efekcie firmy te faktycznie nie reagują na żadne zdarzenia, przez co wartość usług staje się iluzoryczna.

Stworzenie odpowiednich procedur nie jest proste. Na pewno nie można oczekiwać, że zostaną one zaoferowane przez firmy sprzedające rejestratory i kamery. Nie zaoferują ich również firmy tworzące oprogramowanie do obsługi zdarzeń wykrywanych przez systemy wizyjne. W tej chwili możliwe jest tylko wypracowanie ich wspólnie z klientem, u którego zmieniany jest model ochrony. Innych bowiem procedur oczekuje się w przypadku sieci handlowej (kontrola stanowisk kasowych, kontrola przejścia na zaplecze itp.), innych w przypadku hali produkcyjnej (wykrywanie obecności osób postronnych, kontrola

czasu przebywania w magazynie podręcznym itp.), a jeszcze innych w centrum przetwarzania danych (kontrola temperatury pomieszczeń, kontrola obecności drogiego sprzętu itp.). Kwestia procedur związanych z obsługą zdarzeń wykrywanych przez systemy wizyjne zostanie omówiona w osobnym materiale.

Podsumowanie

Moda na zdalny nadzór wizyjny spowodowała, że na rynku pojawił się wysyp usług, które są oferowane w cenach od 20 do 200 zł za kamerę i znacznie różnią się od siebie, co wprowadza wielu klientów w błąd. Mamy więc sprzęt i oprogramowanie, ale brakuje regulaminów dotyczących świadczenia usług, które mogłyby być porównane i uzasadniać koszty.

Brakuje również zróżnicowania praktyk i procedur stosowanych w różnych obiektach. Na zamkniętym osiedlu, w parku maszynowym czy w obiekcie handlowym mogą pojawić się odmienne wyzwania. Dozór wizyjny w przypadku różnych obiektów będzie wymagał innych instrukcji i zaleceń. Liczę na to, że organizacje konsumenckie oraz stowarzyszenia branżowe wpłyną na wypracowanie co najmniej minimalnych regulacji.

W przypadku części firm, które świadczą usługi dozoru wizyjnego, przejawiany jest brak stosownej wiedzy, co widoczne jest w trakcie uruchomień obiektów, gdy obraz z kamery ładuje się kilka minut ze względu na niewłaściwie dobrane łącze. W trakcie eksploatacji systemu, gdy komunikacja z obiektem zostanie przerwana, bo klient zresetuje router, a dostawca usług wyznaczy nowy adres IP, oraz w przypadku sporu z klientem, gdy nie ma dostępu do materiału archiwalnego, gdyż dysk rejestratora zapełnił się w jeden dzień z powodu niewłaściwie dobranych parametrów, trudno zapewnić właściwą ochronę obiektu.

Odnoszę wrażenie, że zmiana modelu ochrony nadeszła zbyt szybko i część firm sobie z tym nie radzi. Niemniej cieszę się, że obecny model wykorzystuje w większym stopniu rozwiązania techniczne, bo doświadczenie i wiedza z dziedziny technicznych zabezpieczeń będzie bardziej doceniana.

Cieszę się również z tego, że na rynku jest kilka firm zajmujących się ochroną, które dostosowały się do zmiany w sposób profesjonalny. Stworzyły opisy świadczonych usług, przygotowały przejrzyste cenniki, wytypowały rozwojowe rozwiązania techniczne, zastosowały zaawansowane programy do obsługi zdarzeń wizyjnych oraz utworzyły zalążki standardowych procedur we współpracy ze swoimi klientami. Firmy te obsługują już po kilka czy kilkanaście tysięcy kamer, więc przetarły trudny szlak.

Powodem do radości jest również to, że tego typu usługi są dostępne w Europie Zachodniej od ponad 30 lat, więc możemy korzystać z doświadczeń firm w krajach, w których koszty ochrony fizycznej są wyższe niż w Polsce. Możemy przygotować się na to, że w ochronie magazynów będą pracowały roboty, a ludzie będą zajmowali się ich programowaniem.

Daniel Kamiński

Alert Control
ALARMY POD KONTROLĄ

ALERTCONTROL Daniel Kamiński
ul. Przyrodnicza 7E
05-126 Michałów-Grabina
alertcontrol@alertcontrol.pl
tel.: (+48) 784 646 386

Advanced
The Standard in Fire Systems

NAJWYŻSZY POZIOM OCHRONY

SYSTEM SYGNALIZACJI POŻARU

Axis EN

ZETO-PROJEKT

WYŁĄCZNY PARTNER FIRMY ADVANCED NA TERENIE POLSKI:
P.U.I. ZETO-PROJEKT SP. Z O. O.
UL. KOLEJOWA 20, 55-075 BIELANY WROCŁAWSKIE
WWW.ZETO-PROJEKT.COM.PL
BIURO@ZETO-PROJEKT.COM.PL

Systemy sygnalizacji pożarowej
w pomieszczeniach elektronicznego przetwarzania danych (część 3)

mgr inż. Jerzy Ciszewski

W pierwszej części artykułu (*Zabezpieczenia* nr 4/2017) wspomniałem, jak ważne jest zabezpieczenie serwerowni. W części drugiej (*Zabezpieczenia* nr 5/2017) opisałem podstawowe źródła zagrożeń pożarowych serwerowni, scharakteryzowałem pożary oraz przedstawiłem kwalifikację pożarową obiektu. W niniejszej części opiszę techniki wykrywania pożaru w serwerowniach

Techniki wykrywania pożaru w serwerowniach

Sposób klimatyzowania obiektu ma wpływ na metodę wykrywania pożaru w serwerowni. Głównym celem wentylacji jest odprowadzenie ciepła (na poziomie ok. 1,5 kW/m^2) wytwarzanego przez działające urządzenia elektroniczne i elektryczne. Są szafy, w których gęstości mocy sięgają 10 kW/m2. Jednym z podstawowych warunków nieawaryjnej pracy tych urządzeń jest utrzymanie stałej wartości temperatury na poziomie ok. 22°C i wilgotności na poziomie ok. 45%. Realizuje to system klimatyzacji precyzyjnej.

Urządzenia elektroniczne są zainstalowane w specjalnych 19" szafach np. typu rack o wysokościach do 42U, dlatego najczęściej stosowanym sposobem wykrywania pożaru jest detekcja dymu zawartego w powietrzu chłodzącym układy elektroniczne zainstalowane w szafie. W zależności od konfiguracji szafy (przód/tył/góra otwarty/zamknięty o prześwicie 80%), przepływ powietrza chłodzącego będzie różny i różny w związku z tym będzie sposób nadzorowania – wykrywania dymu.

Ze względu na przewidywany, najczęściej bezpłomieniowy, rozwój pożaru, a także silną wentylację przyjmowanie typowych powierzchni dozorowania stosowanych w większości obiektów budowlanych nie jest zasadne. Rozchodzenie się dymu ku stropowi w postaci pióropusza w większości przypadków nie ma miejsca.

Do detekcji dymu można wykorzystać:

1) Czujki zainstalowane wewnątrz szafy. Z powodów, które podano wcześniej, taki sposób nadzoru może dotyczyć jedynie przypadku, gdy w szafach znajdują się różne urządzenia elektryczne lub elektroniczne wbudowywane kolejno. W rzeczywistości jako czujka wykorzystywany jest otwór próbkujący rury systemu zasysającego wprowadzonej do wnętrza szafy. Takie rozwiązanie nie powoduje jakichkolwiek obustronnych oddziaływań elektromagnetycznych między urządzeniami elektronicznymi a czujką.
2) Czujki kontrolujące powietrze wylotowe (z szafy).
3) Czujki kontrolujące powietrze wlotowe (do klimatyzatorów).
4) Czujki kontrolujące strefy podpodłogowe, przestrzeń główną, przestrzeń międzystropową w pomieszczeniu, w którym zainstalowane są szafy.

Podłoga podniesiona jest zwykle stosowana z dwóch powodów:
– umożliwienie wykorzystania przestrzeni podpodłogowej do doprowadzania schłodzonego przez klimatyzatory powietrza przez kratki wentylacyjne bezpośrednio pod szafy lub w ich pobliże,
– umożliwienie prostego rozprowadzania przewodów instalacji elektrycznej, telekomunikacyjnej itp.

Z kolei strop podwieszony jest wykorzystywany głównie jako odprowadzenie z pomieszczenia ogrzanego powietrza i skierowania go do systemu klimatyzacji precyzyjnej. Tu również mogą być prowadzone instalacje elektryczne.

Można wyszczególnić kilka sposobów odprowadzania ciepła i utrzymania wymaganych parametrów klimatycznych:

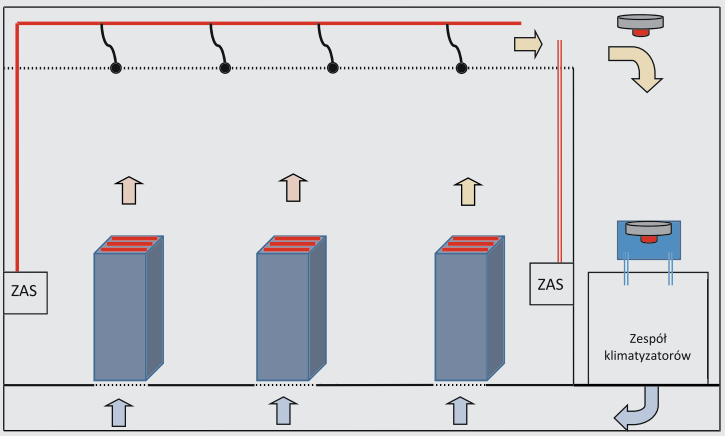
a. Chłodzenie szaf poprzez wentylowanie całej przestrzeni serwerowni;

b. Zastosowanie klimatyzatorów ustawianych w rzędzie z szafami elektroniki. W takim przypadku pojedynczy klimatyzator obsługuje jedną lub dwie szafy, umieszczone po obu jego stronach;
c. Zastosowanie indywidualnego urządzenia chłodzącego w szafie. Rozwiązań jest wiele. Zwykle w szafach z elektroniką znajdują się chłodnice z wentylatorami. Są one połączone orurowaniem z głównym agregatem klimatyzatora obsługującym wiele szaf;
d. Podział obszaru pomieszczenia z szafami, na strefy chłodu i gorąca.

Klimatyzowanie – chłodzenie szaf serwerów poprzez wentylowanie całej przestrzeni serwerowni

Koncepcja 1

Zabezpieczanie serwerowni poprzez chłodzenie całego pomieszczenia z wykorzystaniem wymuszonego przepływu powietrza było stosowane przed laty nawet w dużych serwerowniach. Aktualnie stosuje się je najczęściej w małych obiektach. Wymaga dużej liczby wymian powietrza – w niektórych przypadkach 50 wymian na godzinę. Poszczególne szafy są schładzane również w wyniku działania indywidualnych wentylatorów.



Rys. 1. Koncepcja 1 – zabezpieczenie serwerowni z wykorzystaniem systemu wentylacji mechanicznej

Intensywna wentylacja wymusza prędkości przepływu powietrza sięgające w zależności od miejsca od 0,2 m/s do 15 m/s, a nawet więcej.

Ze względu na dozorowanie całej przestrzeni serwerowni, w której na skutek intensywnej wentylacji dym jest praktycznie równomiernie rozprzestrzeniony, nie jest możliwe wykrycie zagrożonego pożarem urządzenia.

Problemem jest silne rozrzedzenie dymu w pomieszczeniu. Przy określonym rozwoju pożaru dym wytworzony w małej przestrzeni może być z powodzeniem wykryty przez czujki punktowe o czułości rzędu D=5÷10%/m. Jednak w przypadku dużej ilości wymian powietrza, przy silnym rozcieńczeniu dymu, pożar na takim samym etapie rozwoju wymaga wielokrotnie większych czułości czujek – D=0,01÷0,001%/m. Takie czułości są w stanie zapewnić praktycznie jedynie czujki/systemy zasysające.

Nadzorowanie przestrzeni serwerowni

Serwerownię zabezpiecza się za pomocą dwóch systemów zasysających. Pierwszy z nich nadzoruje przestrzeń główną.

Rurki zasysające równomiernie rozmieszcza się na całej powierzchni stropu właściwego. Rurki do pneumatycznego transportu dymu instaluje się w przestrzeni międzystropowej, a smoczki/

Fot. 1. Nadzorowanie przestrzeni głównej w serwerowni z wykorzystaniem systemu zasysającego zainstalowanego w przestrzeni międzystropowej

kapilary zasysające z otworami próbkującymi – w stropie podwieszonym. Przepływy powietrza w poszczególnych gałęziach są zrównoważone. Gwarantuje to stałość czułości poszczególnych otworów próbkujących. Rozmieszczenie otworów próbkujących (zasysających) powinno być zgodne z wytycznymi zawartymi w DTR czujki. Uwzględnia się również wymagania odnoszące się do dopuszczalnej powierzchni dozorowania lub zasięgu, które są zawarte w wytycznych dotyczących projektowania czujek zasysających. Przyjmuje się, że zasięgi są takie jak dla czujek dymowych punktowych.

System zasysający (oznakowany na fotografii 2 strzałkami koloru czerwonego) składa się z rurek zasysających, których otwory próbkujące

umieszczone zostały w pobliżu otworów wlotowych systemu wentylacji serwerowni. Jak widać na fotografii, otwory zasysające są zwrócone w stronę napływającego powietrza. Nie jest to polecane rozwiązanie, ze względu na występujące silne nadciśnienie przy wlocie do rurki. Optymalną konfiguracją jest zastosowanie pewnego kąta odchylenia (ok. 45^0) osi otworu względem wektora prędkości napływającego powietrza. W takim przypadku na czas transportu próbki dymu ma wpływ jedynie wentylator czujki. Na fotografii 2 pokazano również rurkę (oznaczoną żółtą strzałką) zasysającą próbki powietrza, zainstalowaną bezpośrednio na wlocie systemu wentylacyjnego.

Fot. 2. Nadzorowanie przestrzeni międzystropowej

Usytuowanie pojedynczych otworów próbkujących (rurki ucięte pod kątem, tak jak w osłonach przeciwwietrznych) na brzegu wlotowego kanału wentylacji jest niewłaściwe ze względu na silne turbulencje strumienia powietrza, jakie występują na wlocie. Prawidłowym rozwiązaniem jest zastosowanie kilku otworów zasysających, zwróconych w stronę napływającego powietrza, zgodnie z zasadą (0,2–0,4) m^2 powierzchni wlotu powietrza na otwór zasysający.

Celem wyeliminowania fałszywych alarmów zastosowano koincydencję zadziałania dwóch czujek zasysających. Sygnał koincydencji wykorzystany jest do wyzwolenia procedury automatycznego gaszenia. Zaistnieje on wówczas, gdy obie czujki (systemy) zasysające będą w stanie alarmu pożarowego. Sygnał koincydencji będzie rozpoznany przez centralę sygnalizacji pożarowej i zainicjuje ona uruchomienie gaszenia. Aby wyeliminować fałszywe alarmy mogące niezasadnie uruchomić gaszenie, zostały zróżnicowane czułości układów pomiarowych obu czujek zasysających. Taka metoda eliminacji fałszywych alarmów jest skuteczna i prawidłowa.

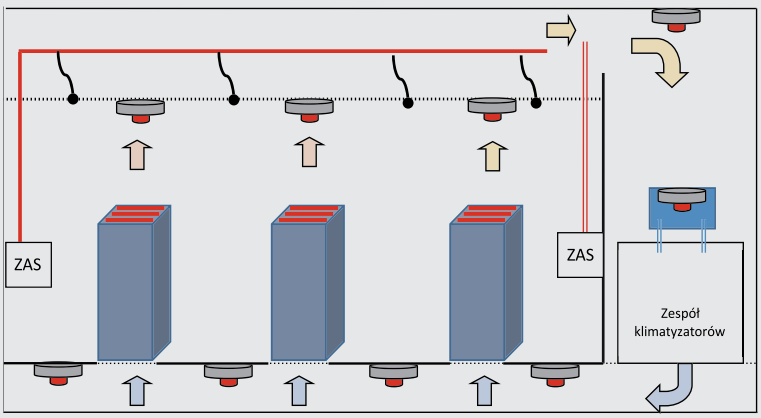
Klimatyzatornia jest nadzorowana przez punktowe optyczne czujki dymu, a czasem (w dużych obiektach) za pomocą liniowej czujki dymu. Do nadzoru kanałów wentylacyjnych stosowane są czujki punktowe w osłonach przeciwwietrznych.

Fot. 3. Czujka w osłonie przeciwwietrznej zainstalowana na wlocie do klimatyzatora

Koncepcja 2

Często stosowanym rozwiązaniem jest konfiguracja z czujkami zasysającymi oraz punktowymi czujkami dymu. Koncepcja nadzoru polega w tym przypadku na wykryciu pożaru przy możliwie dużej czułości detekcji przez system zasysający, który kontroluje przestrzeń główną i (lub) otwory wlotowe systemu wentylacyjnego. Oczywiście w tym przypadku nie jest możliwe zidentyfikowanie zagrożonego pożarem miejsca. W celu wskazania zagrożonej szafy (lub grupy szaf) należy na pewien czas wyłączyć wentylację ogólną w serwerowni. Oczywiście ten czas zależy od ilości ciepła emitowanego przez szafy komputerowe, a także od czasu wybiegu wentylatorów systemu wentylacyjnego. W tym czasie każda szafa jest schładzana przez indywidualny, zainstalowany

w niej wentylator. W takiej sytuacji możliwe jest wyrzucenie zadymionego powietrza z szafy do bezpośredniego otoczenia adresowalnych czujek rozmieszczonych na stropie, dzięki czemu można choćby w przybliżeniu określić, która szafa jest zagrożona. Takie rozwiązanie jest możliwe, jeżeli w szafie a detektorem pożaru. Wysoka czułość wynika przede wszystkim z faktu bezpośredniego zasysania próbek powietrza z szaf. Nie występuje tu zjawisko mieszania powietrza zasysanego z szafy z powietrzem z otoczenia.



Rys. 2. Alarm I stopnia – system zasysający. Alarm II stopnia – czujki punktowe

Fot. 4. Sposób montażu czujki nadzorującej przestrzeń podpodłogową

w serwerowni stosuje się szafy z wylotami wentylacyjnymi na górze. Po wyzwoleniu alarmu II stopnia przywraca się chłodzenie w serwerowni za pomocą wentylacji ogólnej.

Przy rozmieszczaniu czujek w wentylowanej przestrzeni podpodłogowej należy (zgodnie z wytycznymi projektowania WP-02:2010 opracowanymi przez SITP) przyjmować powierzchnię dozorowania nawet trzykrotnie mniejszą niż w przypadku pomieszczeń wysokich – oczywiście przy dostatecznej wentylacji. Według innych wytycznych (np. prTS 54-14) redukcja powierzchni nie jest wymagana.

Indywidualne nadzorowanie szaf

W celu uzyskania największej czułości systemu wykrywania pożaru, można wprowadzić kapilary systemu zasysającego bezpośrednio do wnętrza szaf telekomunikacyjnych. Tego rodzaju rozwiązanie charakteryzuje się brakiem wzajemnych oddziaływań elektromagnetycznych między urządzeniami elektronicznymi zainstalowanymi

W celu poprawienia skuteczności identyfikacji zagrożonych pożarem szaf, na ramionach rurociągu zasysającego są stosowane punktowe czujki adresowalne (należące do tego samego systemu), tak jak pokazano na rysunku 3.

Klimatyzacja serwerowni wykorzystująca techniki zimnych i gorących korytarzy

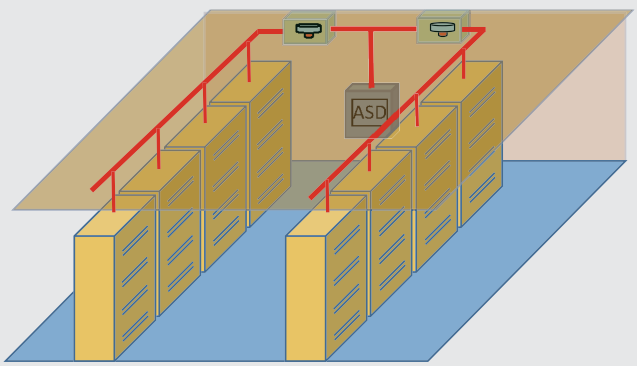
Najczęściej stosowanymi systemami wentylacji w aktualnie eksploatowanych serwerowniach są odmiany wykorzystujące techniki zimnych i gorących korytarzy. Jak widać na rysunku 4, klimatyzatory nadmuchują zimne powietrze do przestrzeni podpodłogowej. Z przestrzeni podpodłogowej zimne powietrze z korytarza zimnego jest przemieszczane przez chłodzone szafy do korytarza gorącego i następnie zasysane do klimatyzatorów. Cykl się powtarza. W porównaniu z poprzednio omawianym sposobem wentylacji liczba wymian powietrza jest znacznie niższa (maksymalnie kilka na godzinę).

Na rysunku 4 pokazane są typowe lokalizacje punktów zasysających próbki powietrza.

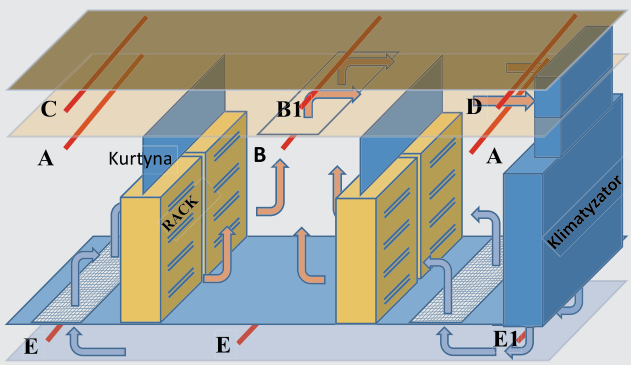
E1 Pod podniesioną podłogą. Nadzorowanie powietrza wylotowego z klimatyzatora ze względu na duże szybkości przepływu, wymaga ustawianie otworów zasysających pod kątem 20-45° do kierunku przepływu powietrza.

Powierzchnia nadzorowanej jednym otworem próbkującym kratki wentylacyjnej – jak wyżej. Kąt ustawienia otworów próbkujących jak wyżej.

Na rysunkach 4 i 5 pokazano różne konfiguracje nadzorowania.



Rys. 3. Nadzorowanie poszczególnych szaf za pomocą systemu zasysającego wykorzystującego rurki kapilarne oraz dodatkowe czujki punktowe w celu identyfikacji grupy szaf



Rys. 4. Zasada nadzoru szaf w przypadku zastosowania klimatyzacji serwerowni wykorzystującej techniki zimnych i gorących korytarzy

E Pod podniesioną podłogą. Nadzorowanie instalacji elektrycznych prowadzonych w tej przestrzeni.

A Nadzorowanie zimnego korytarza.

B Nadzorowanie gorącego korytarza służy do wykrywania pożaru z szafach telekomunikacyjnych, z których powietrze (wraz z dymem) jest wyprowadzane.

B1 Nadzorowanie powietrza napływającego z gorącego korytarza. Na skutek silnego mieszania się powietrza gorącego z chłodnym, zalegającym przestrzeń międzystropową następuje zmniejszenie czułości detekcji, a także pogorszenie identyfikacji miejsca zagrożenia. Pojedynczy otwór zasysający powinien nadzorować kratkę wentylacyjną o powierzchni nie większej niż 0,4 m^2 .

C Nadzorowanie przestrzeni międzystropowej. Zagrożenie pożarem związane z gęstością obciążenia ogniowego, wynikającego z ilości i rodzaju zainstalowanych tam kabli elektrycznych.

D Powrót powietrza wentylującego serwerownię.

Dym jest wykrywany przez system zasysający, pobierający próbki:
- gorącego powietrza dostającego się do klimatyzatorów,
- powietrza dostającego się do systemu wentylacyjnego całego pomieszczenia (wentylacji ogólnej),
- powietrza z przestrzeni pod podniesioną podłogą.

Głównym problemem jest brak możliwości ustalenia, która jednostka jest zagrożona pożarem. Dym zasysany przez czujkę zasysającą może pochodzić z wielu jednostek, gdyż powietrze w korytarzu gorącym jest silnie wymieszane.

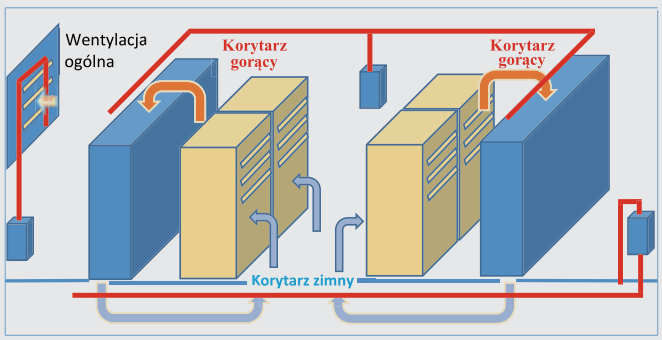
Rozwinięciem koncepcji jest zastosowanie korytarzy krytych pokazanych na rysunku 6. Dzięki nim efektywność systemu chłodzącego jest znacznie wyższa niż w poprzedniej wersji.

Sposób wykrywania pożaru jest analogiczny do rozwiązania poprzedniego. Również w tym przypadku do detekcji wykorzystuje się powietrze wprowadzane do jednostek klimatyzatorów, zawierające już silnie rozrzedzony dym. Może to skutkować opóźnioną detekcją pożaru.

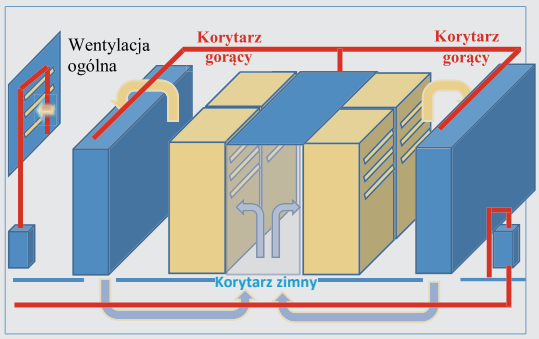
Kolejna odmiana systemu wentylacji wykorzystuje konfigurację zamkniętej od dołu i po bokach oraz otwartej od góry przestrzeni gorącego korytarza. W serwerowni może być kilka takich struktur („kiosków"). Chłodne powietrze z klimatyzatorów jest tłoczone do przestrzeni podpodłogowej, a następnie zasysane do szaf serwerowych. Gorące powietrze wydostaje się z szaf, przedostaje do przestrzeni między szafami, a następnie przemieszcza się do przestrzeni międzystropowej. Stamtąd trafia do szaf klimatyzatorów.

Zazwyczaj próbki powietrza są pobierane znad szaf klimatyzatorów, co nie jest najlepszym rozwiązaniem, gdyż znieczula system wykrywania pożaru na skutek silnego mieszania powietrza. Znacznie bardziej skuteczne jest pobieranie próbek powietrza z górnej części „kiosku" za pomocą systemu zasysającego zaznaczonego na rysunku 7 kolorem zielonym. W takim przypadku miejsce wystąpienia pożaru jest identyfikowane z dokładnością wynikającą z liczby szaf stanowiących strukturę „kiosku".

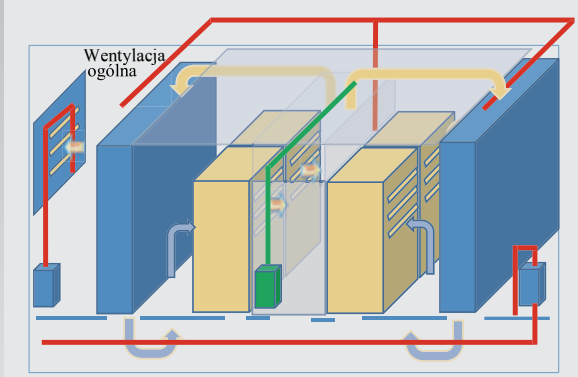
W aktualnie budowanych serwerowniach, w których urządzenia elektryczne i elektroniczne są schładzane na wyżej wymienione sposoby, system wentylacji schładzającej nie jest wyłączany po wykryciu pożaru. W przypadku uruchomienia stałych urządzeń gaśniczych wyłączana jest jedynie wentylacja ogólna.



Rys. 5. Klimatyzacja wykorzystująca technikę zimnych i gorących korytarzy



Rys. 6. Technika krytych korytarzy



Rys. 7. Zastosowanie konfiguracji „kiosków"

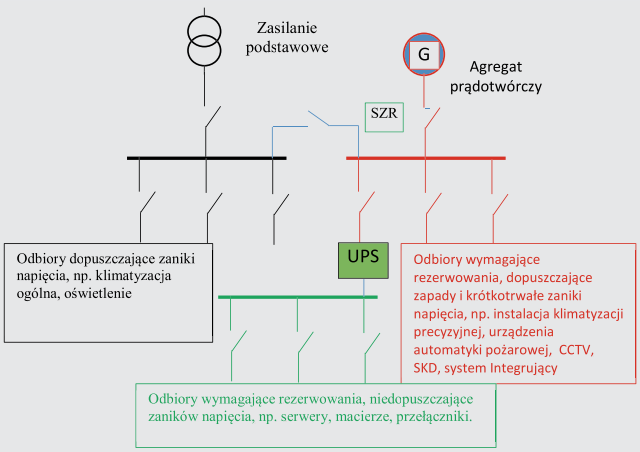
Fot. 5. Brak skutecznego nadzoru agregatu prądotwórczego

Zabezpieczenie generatora prądotwórczego

Jak wcześniej powiedziano, jednym z czynników gwarantujących ciągłą i niezawodną pracę systemów informatycznych, jest zapewnienie bezpiecznego, bezprzerwowego zasilania. Dlatego system zasilania charakteryzuje się silną nadmiarowością.

Wydzielone pożarowo pomieszczenie, w którym znajduje się generator i zapas paliwa do niego, powinno być nadzorowane przez minimum dwie pracujące w podczerwieni czujki płomieni (4,3 µm) umieszczone przeciwlegle po obu stronach generatora tak, aby mogły nadzorować całe pomieszczenie i generator. Czujki płomieni nie są w stanie wykryć pożarów pirolitycznych, powstałych na skutek przegrzewania się układów

Fot. 6. Czujka płomieni nadzorująca agregat prądotwórczy



Rys. 8. Uproszczony schemat zasilania odbiorów elektrycznych serwerowni

Agregaty prądotwórcze w centrach przetwarzania danych stanowią zwykle zapasowe źródła energii elektrycznej, uruchamiane w przypadku braku zasilania podstawowego, a więc na skutek wykrycia zaniku napięcia w sieci. Rozruch agregatu trwa od kilkunastu do kilkudziesięciu sekund, dlatego do momentu ustabilizowania pracy i przejęcia obciążenia odbiorniki serwerowni są zasilane przez zasilacze UPS wyposażone w baterie akumulatorów o odpowiedniej pojemności. Z agregatem współpracuje układ samoczynnego załączania rezerwy (SZR), który ma wykryć zanik napięcia, uruchomić agregat, a następnie, po ustabilizowaniu pracy, przyłączyć agregat do odpowiedniego pola rozdzielni elektrycznej.

Warto przypomnieć, że agregaty będące źródłami zapasowego zasilania systemów różnicowania ciśnienia zwykle są uruchamiane na skutek wykrycia pożaru tak, aby nie było dodatkowego opóźnienia w działaniu tych systemów wynikającego z czasu uruchamiania agregatu.

elektrycznych i elektronicznych układów sterowniczych generatora, dlatego zasadne jest zainstalowanie w pomieszczeniu punktowej optycznej czujki dymu.

Bardzo często pomieszczenie (zwykle kontener) zabezpiecza się za pomocą stałego urządzenia gaśniczego.

W części 4 napiszę o zabezpieczeniu transformatorów, UPS-ów i akumulatorni.

mgr inż. Jerzy Ciszewski
IBP NODEX

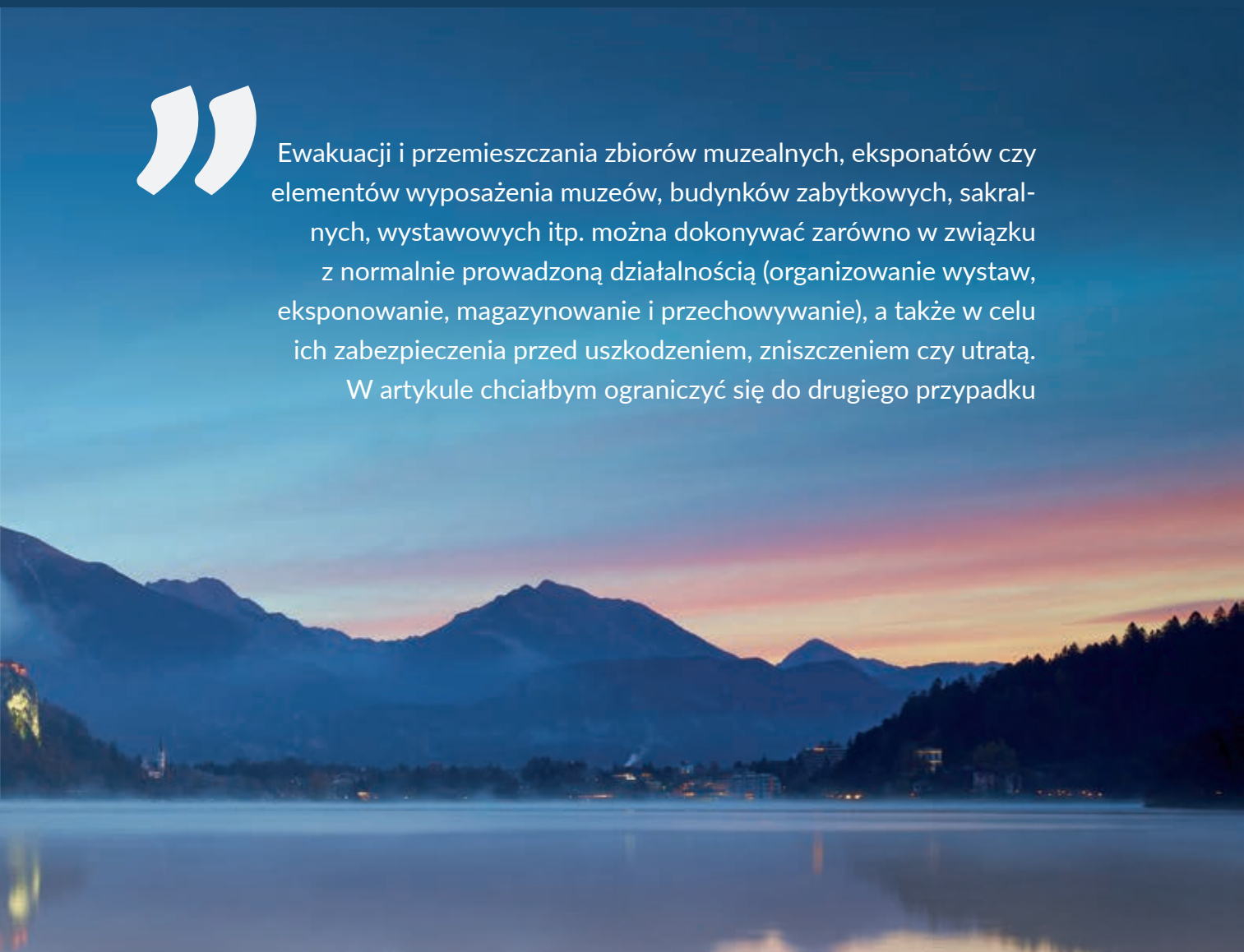
Ochrona obiektów zabytkowych i zbiorów muzealnych

przed pożarem lub zalaniem

Arkadiusz Milka

Są dwa główne zagrożenia, które powodują konieczność ewakuacji zbiorów najczęściej – zagrożenie pożarem oraz zagrożenie zalaniem. Jednoznacznie potwierdzają to statystyki. W przypadku pożaru albo zalania pierwszym i podstawowym zadaniem właściciela obiektu lub zarządcy nieruchomości jest natychmiastowa ewakuacja ludzi ze stref, w których zagrożone jest ich zdrowie lub życie. Wymagania z tym związane są szczegółowo uregulowane przez odpowiednie przepisy, zwłaszcza Prawo Budowlane oraz przepisy dotyczące ochrony przeciwpożarowej. Wymagania dotyczące ewakuacji zbiorów w przypadku zagrożenia reguluje z kolei rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 2 września 2014 roku w sprawie zabezpieczenia zbiorów muzealnych przed pożarem, kradzieżą i innymi niebezpieczeństwami grożącymi ich zniszczeniem lub utratą (Dz. U. z 2014 r., poz. 1240). Ponadto muzea zostały zobowiązane do opracowania i wprowadzenia do połowy 2015 roku instrukcji przygotowania zbiorów do ewakuacji.

W celu podjęcia decyzji o ewakuacji osób czy zbiorów w przypadku zagrożenia konieczne jest odpowiednio wczesne jego wykrycie i powiadomienie o nim osób i służb odpowiedzialnych za bezpieczeństwo. Kiedy ewakuacja jest niezbędna? Najczęściej wówczas, gdy powstałe zagrożenie osiąga (lub istnieje duże prawdopodobieństwo, że osiągnie) taką skalę i rozmiary, że nie będzie możliwe jego opanowanie. Kiedy najczęściej dochodzi do tak niebezpiecznej sytuacji? Wówczas, gdy powstałe zagrożenie nie zostało odpowiednio wcześnie wykryte i zasygnalizowane lub powstało bardzo gwałtownie. W efekcie dochodzi do niekontrolowanego rozwoju zdarzeń, któremu trudno lub wręcz nie można przeciwdziałać.



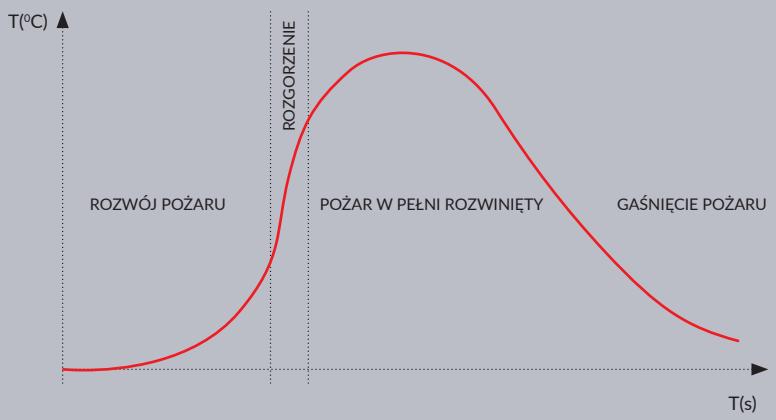
> Ewakuacji i przemieszczania zbiorów muzealnych, eksponatów czy elementów wyposażenia muzeów, budynków zabytkowych, sakralnych, wystawowych itp. można dokonywać zarówno w związku z normalnie prowadzoną działalnością (organizowanie wystaw, eksponowanie, magazynowanie i przechowywanie), a także w celu ich zabezpieczenia przed uszkodzeniem, zniszczeniem czy utratą. W artykule chciałbym ograniczyć się do drugiego przypadku

Jedną z najważniejszych metod przeciwdziałania pożarowi i zalaniu oraz ograniczania ich skutków jest wyposażenie obiektów w odpowiednią infrastrukturę, tj. urządzenia techniczne umożliwiające odpowiednio wczesne wykrycie powstałego zagrożenia.

W ostatnich latach można było dostrzec bardzo duży postęp w tym zakresie. Obecnie mamy do dyspozycji liczne rozwiązania, które umożliwiają skuteczne i bardzo wczesne wykrycie oraz automatyczne ograniczenie, a nawet zneutralizowanie wielu rodzajów zagrożeń. W przypadku wykrywania pożaru albo zalania każda sekunda jest dosłownie na wagę złota i decyduje o skuteczności późniejszych działań ratowniczych. W związku z tym bezwzględnie powinniśmy wykorzystywać wszelkie możliwości techniczne i organizacyjne. Jeżeli zapewnimy odpowiedni czas na wykrycie zagrożenia, możliwa będzie lepsza ochrona zbiorów przed ich nieodwracalnym uszkodzeniem, zniszczeniem czy utratą.

W przypadku pożaru najważniejsze jest wykrycie go w bardzo wczesnej fazie, czyli w fazie tlenia lub wzrostu temperatury ponad normę, czyli wówczas, gdy jeszcze nie powstał otwarty ogień i nie nastąpiło jego rozgorzenie. Najlepiej ilustruje to wykres faz rozwoju pożaru przedstawiający wzrost temperatury w funkcji czasu. Jeżeli pozwolimy na niekontrolowany rozwój pożaru, który osiągnie stan rozgorzenia, to szanse na jego opanowanie i uratowanie obiektu (strefy pożarowej) są praktycznie równe zeru.

Warto podkreślić, iż obecnie dostępne są nowoczesne rozwiązania, które umożliwiają wykrycie pożaru w bardzo wstępnej fazie. Z kolei rozwój systemów i technik bezprzewodowych stworzył dodatkowo możliwość instalowania systemów detekcji pożaru bez konieczności układania okablowania, a w związku z tym bez potrzeby ingerencji w strukturę zabytkowego obiektu. Wcześniej instalowanie systemów wykrywania pożaru w tego rodzaju obiektach bardzo często



Rys. 1. Przebieg pożaru w funkcji czasu T=f(t)

było praktycznie niemożliwe ze względu na ograniczenia techniczne czy konserwatorskie.

Podobnie jest w przypadku zagrożenia zalaniem. Tylko wczesne wykrycie źródła wycieku umożliwia ograniczenie jego skutków. Trzeba pamiętać, że często bardzo duże straty są spowodowane przez z pozoru drobne i niegroźne wycieki, które nie zostały odpowiednio wcześnie wykryte. Zabytkowe budynki są szczególne zagrożone zalaniem z powodu złego stanu technicznego funkcjonujących od wielu lat instalacji. Duże zagrożenie stwarzają także wszechobecne instalacje klimatyzacyjne, hydrantowe, gaśnicze, wodne i kanalizacyjne, nierzadko przebiegające przez pomieszczenia, w których eksponowane lub magazynowane są zbiory. Zagrożenie zalaniem w pomieszczeniach magazynowych może trwać przez wiele godzin, a nawet dni, jako że najczęściej są to pomieszczenia zamknięte i niemonitorowane, a w niektórych obiektach nie ma całodobowego nadzoru czy obsługi. Ponadto dostęp do większości pomieszczeń, w których przechowywane czy magazynowane są zbiory, jest możliwy dopiero w efekcie określonych procedur, co ma duży wpływ na szybkość reakcji. Wydłuża to znacznie czas weryfikacji zagrożenia, a tym samym utrudnia podjęcie szybkich i skutecznych działań ratowniczo-zapobiegawczych w przypadku jego potwierdzenia.

W przypadku ochrony przeciwpożarowej problem jest prawnie uregulowany, chociaż tylko częściowo. Należy wyraźnie podkreślić, że nie wszystkie obiekty zabytkowe, łącznie z tymi, które stanowią nasze dziedzictwo kulturowe i narodowe, muszą być wyposażone w systemy sygnalizacji pożarowej obejmujące urządzenia sygnalizacyjno-alarmowe służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze odbierające alarmy pożarowe i sygnały uszkodzeniowe. Wymóg taki odnosi się tylko do tych obiektów, które są wymienione w rozporządzeniu Ministra Spraw Wewnętrznych Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów. Zgodnie z § 28.1 ust. 14 w systemy sygnalizacji pożarowej obligatoryjnie powinny być wyposażone „muzea oraz zabytki budowlane wyznaczone przez Generalnego Konserwatora Zabytków w uzgodnieniu z Komendantem Głównym Państwowej Straży Pożarnej". Niestety systemy te nie są instalowane w zagrożonych miejscach, jeżeli zastosowanie ich tam nie jest narzucone przez przepisy.

Niestety żadne przepisy w Polsce nie regulują zastosowania systemów wykrywania wycieków, nawet w odniesieniu do obiektów o szczególnej wartości kulturowej czy materialnej. W efekcie, mimo największych strat wywołanych zalaniami, na dzień dzisiejszy w systemy wykrywania wycieków wyposażane są tylko nieliczne obiekty. Jest to niezrozumiałe tym bardziej, że koszty ich instalacji oraz eksploatacji są relatywnie bardzo niskie.

W kolejnym artykule będę starał się przedstawić sposoby działania oraz techniczne rozwiązania umożliwiające wczesną i skuteczną detekcję zagrożeń pożarem i wyciekami.

Arkadiusz Milka
rzeczoznawca ds. zabezpieczeń technicznych
i zarządzania bezpieczeństwem

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

dobrze zaprojektowane BEZPIECZEŃSTWO

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

oraz

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

Komunikacja bezprzewodowa
w systemach alarmowych

Michał Konarski

> System alarmowy jest rozległą instalacją wymagającą ułożenia dziesiątków metrów okablowania. Z tego powodu nieustannie rosnącym zainteresowaniem cieszą się systemy hybrydowe oraz bezprzewodowe, w których komunikacja pomiędzy poszczególnymi elementami odbywa się drogą radiową

Współczesne systemy łączności bezprzewodowej przeszły długą drogę rozwoju. Wykorzystanie nowych generacji komponentów pozwala zwiększyć niezawodność komunikacji, a także obniżyć zapotrzebowanie na energię, co może przekładać się na dłuższe odstępy pomiędzy wymianami baterii w urządzeniach.

Wyzwania inżynierskie dotyczące komunikacji bezprzewodowej

Dwa główne wyzwania w przypadku komunikacji bezprzewodowej to zapewnienie niezawodnego przesyłania informacji z użyciem ogólnodostępnego medium (fal radiowych z wybranego zakresu częstotliwości) oraz – w przypadku urządzeń działających autonomicznie (bez zewnętrznego źródła zasilania) – energooszczędności. Należy osiągnąć jednocześnie oba wymienione cele, co wymaga kompromisów.

Uzyskanie niezawodnego przekazywania informacji jest trudne, gdy nie ma możliwości odizolowania kanału komunikacyjnego od oddziaływania zewnętrznego. W przypadku tradycyjnych połączeń przewodowych pewność przekazywania

informacji jest bardzo wysoka, natomiast połączenia bezprzewodowe są narażone na celowe lub przypadkowe zakłócenia przekazywania informacji, a także na liczne zjawiska powodujące osłabienie poziomu użytecznego sygnału. Wpływ tych niekorzystnych zjawisk można minimalizować na kilka sposobów – poprzez zwiększenie tzw. budżetu łącza radiowego, wykorzystanie lepszych (bardziej selektywnych) odbiorników i specjalistycznych modulacji, w tym mechanizmów rozpraszania widma radiowego, oraz wprowadzenie mechanizmów nadmiarowości (zwielokrotnionych transmisji czy uzupełnienia przesyłanych informacji tzw. danymi naprawczymi). Wiąże się to z koniecznością użycia lepszych (i najczęściej droższych) układów komunikacyjnych oraz ze zwiększeniem zapotrzebowania na energię.

Z drugiej strony urządzenia powinny mieścić się w niewielkich obudowach i pracować jak najdłużej, najlepiej przez wiele lat.

Systemy transmitujące sygnały jednokierunkowo lub dwukierunkowo

Najprostszym rozwiązaniem jest zastosowanie niesymetrycznego toru komunikacji radiowej – wyposażenie czujek alarmowych w nadajnik radiowy, a centrali alarmowej w odpowiedni odbiornik. Taki sposób komunikacji pozwala na przesłanie informacji o zadziałaniu czujki, lecz nie daje możliwości przekazania żadnej informacji zwrotnej. W przypadku transmisji jednokierunkowej czujki „nie wiedzą", czy informacja o alarmie dotarła do odbiornika, więc – aby zwiększyć prawdopodobieństwo, że taka transmisja się powiedzie – nadawanie jest kilkukrotnie powtarzane. Dzięki temu w sprzyjających warunkach, przy ewentualnych zakłóceniach, o ile są krótkotrwałe, sygnał alarmowy powinien dotrzeć do celu.

Czujki transmitujące jednokierunkowo nie mogą „dowiedzieć się", czy włączono w dozór system lub strefę dozorową. W efekcie, podczas standardowej aktywności w miejscu czasowo wyłączonym z dozoru, gdy wykrywany jest ruch w pomieszczeniach z czujkami ruchu czy otwieranie są drzwi lub okna chronione czujkami kontaktronowymi, przesyłane są nadmiarowe informacje mogące niekorzystnie wpływać na żywotność baterii w czujkach. Sposobem pozwalającym na osiągnięcie akceptowalnych okresów pomiędzy wymianami baterii jest usypianie czujek po wykryciu zdarzenia na określony czas – z reguły kilkuminutowy (a nawet kilkunastominutowy). W ten sposób można zmniejszyć liczbę nadmiarowych transmisji, ale rozwiązanie to ma również bardzo istotne ze względu na bezpieczeństwo reperkusje. Chodzi tu przede wszystkim o scenariusz wyjścia z chronionego obiektu i włączenia systemu w dozór – przez wiele minut systemy z transmisją jednokierunkową, pracujące w trybie oszczędzania baterii, nie zapewniają należytej ochrony.

Ze względu na to, że obecnie jednokierunkowa komunikacja stosowana jest praktycznie wyłącznie w sprzęcie co najwyżej półprofesjonalnym, pojawia się w tych urządzeniach szereg innych uproszczeń. Proste systemy z transmisją jednokierunkową pracują w pasmie częstotliwości 433 MHz z wykorzystaniem prostej modulacji amplitudy (podobnej do tej wykorzystywanej dawniej w rozgłośniach radiowych na falach długich i średnich). Ten zakres częstotliwości jest powszechnie wykorzystywany przez proste urządzenia radiowe – piloty do zdalnego sterowania, bezprzewodowe dzwonki i inne tego typu produkty. Również duża część odbiorników, ze względu na przyjęte uproszczenia, pozostawia wiele do życzenia pod względem selektywności (czyli zdolności do odróżnienia sygnałów użytecznych od zakłócających) czy czułości.

Rozwój półprzewodników umożliwił skuteczne zastosowanie komunikacji dwukierunkowej w sprzęcie alarmowym. Wyposażenie każdego urządzenia w nadajnik oraz odbiornik daje wiele korzyści. Podstawową korzyścią jest możliwość potwierdzenia odebrania sygnału, które znacznie poprawia niezawodność przesyłania informacji. Przy braku potwierdzenia (np. z powodu zakłócenia transmisji) komunikat może być wielokrotnie powtórzony bez istotnego wpływu na zużycie energii. Dodatkowo czujki transmitujące dwukierunkowo mogą odbierać informacje o włączeniu systemu w dozór, odpowiednio dostosowując strategię komunikacji do aktualnych warunków. Dzięki temu możliwe jest znaczne ograniczenie zużycia energii, którą można wykorzystać w celu poprawienia szybkości reakcji systemu na zdarzenia (np. skracając interwały komunikacyjne) lub wydłużenia czasu autonomicznej pracy urządzeń bezprzewodowych. Przekazywanie informacji o stanie czuwania ma również związek z przyspieszeniem włączania systemu w dozór, czyli skróceniem czasu, przez który system nie reaguje na zdarzenia. W efekcie jest on znacznie bardziej bezpieczny.

Inną korzyścią z dwukierunkowej komunikacji jest możliwość zdalnego konfigurowania urządzeń – np. zmiany czułości czujki PIR czy aktywacji tzw. WalkTestu bez konieczności fizycznego dostępu do czujki.

Nowoczesne układy komunikacyjne nie tylko umożliwiają dwukierunkową komunikację. Wykorzystanie ich możliwości zbiegło się z przejściem na pasmo częstotliwości 868 MHz. O ile inna częstotliwość nie jest ani lepsza, ani gorsza, fakt narzucenia przez urzędy regulacyjne bardziej restrykcyjnych przepisów dotyczących dostępu do tej części pasma radiowego powoduje, że jest ona dużo mniej zaśmiecona, a w związku z tym transmisja jest pewniejsza. Urządzenia alarmowe transmitujące dwukierunkowo korzystają też powszechnie z bardziej zaawansowanych metod modulacji, które są bardziej odporne na zakłócenia.

Rozbudowane i zaawansowane odbiorniki, stosowane zwłaszcza w urządzeniach nowszej generacji, cechują się dobrą selektywnością oraz czułością. W efekcie urządzenia wykorzystujące taką technikę transmisji są bardziej złożone i wyprodukowanie ich jest droższe, ale korzyści płynące z ich zastosowania z nawiązką rekompensują wyższą cenę.

Cała prawda o zasięgu

Jednym z najczęściej branych pod uwagę parametrów urządzeń bezprzewodowych jest zasięg łączności radiowej. Wynika to w dużej mierze z dotychczasowych doświadczeń instalatorów systemów zabezpieczeń. Słysząc o zasięgach rzędu 100 m, 200 m i 300 m, instalatorzy zakładali, że realny dystans kilku czy kilkunastu metrów pomiędzy urządzeniami będzie gwarantował dobrą jakość komunikacji (w końcu sprzęt powinien dysponować rezerwą zasięgu). Niestety tak nie było, zwłaszcza w przypadku zastosowania mniej wyrafinowanych urządzeń. Producenci i dystrybutorzy, pod presją oczekiwań swoich klientów, zaczęli podawać coraz bardziej wyśrubowane parametry opisywane jako zasięg w terenie otwartym.

Owszem, zasięg w terenie otwartym to istotny parametr określający budżet energetyczny połączenia pomiędzy nadajnikiem i odbiornikiem (zależność związaną z mocą nadajnika i czułością odbiornika). Nie umożliwia on jednak jednoznacznego określenia, jak dobrze dane urządzenia poradzą sobie w realnych warunkach instalacyjnych. Dwa systemy o identycznym zasięgu mierzonym w terenie otwartym mogą zupełnie różnie zachować się w realnym obiekcie. Wynika to z faktu, że pomiary zasięgu w przestrzeni otwartej nie uwzględniają potencjalnych źródeł zakłóceń, zjawisk odbicia i wygaszania sygnału, a także skupiają się wyłącznie na przypadku optymalnego położenia anten. W rzeczywistej sytuacji pojawiają się przeszkody stałe: ściany, stropy, nierzadko solidnie zbrojone czy wyposażone w dziesiątki metrów kabli. Pojawiają się źródła zakłóceń: pracujące urządzenia elektryczne i elektroniczne, a także inne urządzenia komunikujące się bezprzewodowo. Poza tym poszczególne urządzenia są montowane w miejscach narzuconych przez zasadę działania (np. czujki ruchu powinny być zamontowane w określonym miejscu, by swoim polem detekcji objąć chroniony obszar), niekoniecznie tam, gdzie byłoby to korzystne ze względu na łączność radiową. Do tego dochodzą czynniki zmienne – ludzie w pomieszczeniach (dla fal z zakresu setek MHz ciało ludzkie stanowi przeszkodę) czy ruchome meble lub towary na półkach magazynowych.

Czynników wpływających na skuteczność łączności jest bardzo dużo. Praktycznie nie sposób określić nawet w dużym przybliżeniu, jaką komunikację uzyskamy pomiędzy punktem A i punktem B

w konkretnym budynku, dlatego w każdym innym niż akademickie rozważania przypadku niezbędne będzie praktyczne zweryfikowanie osiągów urządzeń. W tym celu producenci zaawansowanych urządzeń bezprzewodowych dają instalatorom stosowne narzędzia – skanery pasma czy testery pozwalające mierzyć poziom sygnału. Skaner pasma może dać instalatorowi informację o tym, czy w danej lokalizacji poziom zakłóceń radiowych spowoduje pogorszenie parametrów (osłabienie czułości), oraz umożliwi oszacowanie, w jakim stopniu sygnały z urządzeń (czujek itp.) odróżniają się od szumu tła. Dzięki testerowi mierzącemu poziom sygnału można wybrać optymalne miejsce montażu elementów składowych systemu. Niektórzy producenci oferują czujki wyposażone w zintegrowany tester sygnału, więc nie trzeba kupować odrębnego urządzenia.

Projektując systemy bezprzewodowe, należy brać pod uwagę to, że w przypadku pasma 868 MHz faktyczny zasięg wewnątrz budynków będzie wahać się w granicach od kilkudziesięciu metrów w sprzyjających warunkach (lekka zabudowa – cegła lub ścianki gipsowe, urządzenia zainstalowane na jednej kondygnacji) do kilkunastu czy nawet kilku metrów w trudnych warunkach (ściany żelbetowe, komunikacja przez stropy). Może więc okazać się, że niezbędne będzie użycie urządzeń poprawiających jakość komunikacji – powielaczy sygnału (tzw. repeaterów) czy systemów komórkowych z wieloma modułami odbiorczymi, umożliwiających wybór optymalnej trasy sygnału radiowego.

Wewnątrz pomieszczeń, gdzie występują rozliczne odbicia sygnału radiowego od przeszkód czy lokalne zaniki sygnału, lepiej działają odbiorniki wyposażone w układ wielu anten automatycznie wybierających silniejszy sygnał (tzw. odbiór przestrzennie zbiorczy). W ten sposób można w pewnym stopniu zminimalizować niekorzystny wpływ przeszkód i zapewnić bardziej równomierny zasięg wewnątrz pomieszczeń.

Czy warto stosować techniki bezprzewodowe?

Odpowiedź na to pytanie jest napisana przez życie. W wielu przypadkach bezprzewodowy system alarmowy będzie optymalnym wyborem. Obiekty o wysokim standardzie wykończenia, w przypadku których koszt wykonania prac remontowych nie znalazłby ekonomicznego uzasadnienia, czy budynki, których oryginalnej struktury nie można zmieniać, są typowymi miejscami zastosowania urządzeń bezprzewodowych. Dużą zaletą urządzeń bezprzewodowych jest też szybki montaż – nie trzeba układać okablowania. Nie bez znaczenia jest też rachunek ekonomiczny – zwłaszcza w krajach Europy Zachodniej, w których koszty pracy ludzkiej są na tyle wysokie, że mimo zastosowania droższych i bardziej skomplikowanych komponentów bezprzewodowych całkowity koszt wykonania zabezpieczenia bezprzewodowego będzie niski w porównaniu z systemem tradycyjnym.

Mimo pozornie prostszej instalacji prawidłowy dobór komponentów i ich właściwe skonfigurowanie wymaga wiedzy i doświadczenia. Przydatna jest też wiedza dotycząca ograniczeń zastosowanych technik – niejednokrotnie pozwala ona zrozumieć istotę złożonych zjawisk zachodzących w systemie komunikującym się drogą radiową. Dokonanie odpowiedniego wyboru, a później świadome wykorzystanie dostępnych narzędzi pozwoli zaoszczędzić czas i pieniądze.

Michał Konarski

WIELOPUNKTOWY I WIELOGAZOWY SYSTEM DETEKCJI CO/LPG...NO_2... W GARAŻACH I PARKINGACH PODZIEMNYCH

JEŚLI MUSISZ STOSUJ ORYGINALNE

Uwaga!

Wielogazowe, stacjonarne detektory gazów oraz połączenie dwóch modułów urządzenia to wyłączne i chronione know-how firmy Pro-Service

PRO-SERVICE®

Przedsiębiorstwo Wdrożeniowe Pro-Service© Sp. z o.o.
Os. Złotej Jesieni 4, 31-826 Kraków, Tel. 12 425 90 90
www.alarmgaz.com

Wielofunkcyjne sensory
systemu ochrony obwodowej V-Alert

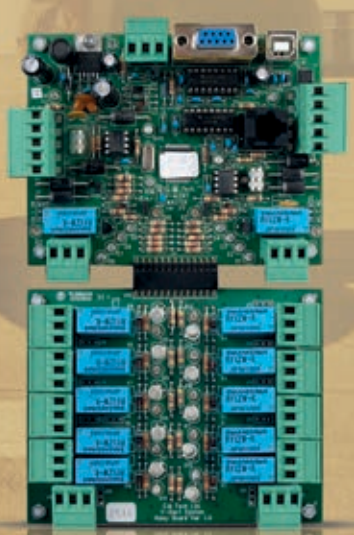
Bartłomiej Kwiatkowski

Zabezpieczenie strefy obwodowej jest wymagane, gdy bezpieczeństwo i niezakłócone funkcjonowanie danego obiektu, infrastruktura lub znajdujące się na danym obszarze mienie mają szczególną ważność lub wartość. Dotyczy to m.in. lotnisk, radarów wykorzystywanych w kontroli ruchu lotniczego, jednostek wojskowych, magazynów wojskowych, więzień, elektrowni itp. W ich przypadku czas reakcji na niepożądane zdarzenia powinien być jak najszybszy, czyli reakcja powinna nastąpić już w momencie naruszenia strefy obwodowej

System V-Alert, o którym będzie mowa w niniejszym artykule, stanowi profesjonalne i wysoce skuteczne zabezpieczenie strefy obwodowej obiektu. Jest to system składający się przede wszystkim z elektronicznych sensorów mikroprocesorowych. Urządzenia te nie zawierają części ruchomych. Wykrywają zmiany położenia lub reagują na wibracje spowodowane przez próby cięcia, niszczenia lub kradzieży elementów chronionych. Sensory do wykrywania zmiany położenia wykorzystują układ półprzewodnikowy zwany akcelerometrem. Wysyła on informację do mikrokontrolera zarządzającego sensorem, a następnie do karty procesorowej. Jest to innowacyjna metoda przekładająca się na bezawaryjną, niezawodną i stabilną pracę całego systemu.

Status każdego sensora jest monitorowany i analizowany w sposób ciągły przez kartę procesorową wykrywającą zmiany stanów poszczególnych sensorów przez porównanie ich ze stanami sensorów sąsiadujących. W rezultacie można dokładnie i wiarygodnie wykrywać stany alarmowe poszczególnych sensorów.

Karta procesorowa umożliwia podłączenie dwóch linii sensorowych, z których każda może zawierać do 50 sensorów. Maksymalna długość linii sensorowej wynosi 800 m. Standardowa odległość między sensorami to 3 m, ale producent umożliwia zamówienie linii sensorowej, na której sensory są oddalone od siebie o 5 m lub 7 m. Jeżeli wymagane są niestandardowe odległości pomiędzy sensorami (np. w przypadku bram, furtek, śluz), stosuje się specjalny przewód i hermetyczne puszki połączeniowe. System może pracować zarówno na zewnątrz, jak i wewnątrz budynków. Spełnia najbardziej restrykcyjne wymagania dotyczące urządzeń czwartej klasy środowiskowej. Karta procesorowa może pracować w temperaturach z zakresu od -30°C do 70°C.



Fot. 1. Karta procesorowa VAPC oraz karta wyjść przekaźnikowych VArelay

Zaletą linii sensorowych dostarczonych przez producenta jest gotowość do instalacji na odpowiednio przygotowanej powierzchni. Ze względu na specyfikę systemu przy składaniu zamówienia przez nabywcę konieczne jest dokładne określenie parametrów linii sensorowych. Wynika to z faktu, że producent w procesie produkcyjnym montuje sensory na linii, sprawdza poprawność ich działania, po czym zalewa je żywicą. Nie stanowi to problemu w przypadku potrzeby rozbudowy systemu czy zmiany jego konfiguracji. Za pomocą odpowiedniego urządzenia można zmienić adresację sensorów (dodać lub podmienić w przypadku uszkodzenia) na linii sensorowej. Tego typu rozwiązanie przynosi korzyści, skraca czas instalacji systemu, zapewnia sprawność urządzeń oraz, co najważniejsze, umożliwia pracę sensorów w najtrudniejszych warunkach atmosferycznych.

Klasa szczelności sensorów to IP67. Mogą one pracować w temperaturach z zakresu od -30°C do 70°C. Przewód wykorzystany do połączenia sensorów ma dwie zewnętrzne warstwy izolacyjne. W konstrukcji przewodu zastosowano włókna kevlarowe zapobiegające jego rozciąganiu. Powłoka zewnętrzna jest odporna na uszkodzenia mechaniczne oraz na oddziaływanie czynników środowiskowych, w tym na promieniowanie UV.

W przypadku każdego z obiektów sensory mogą być wykorzystane na różne sposoby, ponieważ każdy z nich może mieć zdefiniowaną inną czułość. Można je instalować na ogrodzeniach z siatki, paneli zgrzewanych, belek, na ogrodzeniach murowanych oraz na konstrukcjach stałych, takich jak dachy, konstrukcje metalowe, wieże. Sensory mogą również wykrywać próby kucia i przebijania się przez ściany, a także zabezpieczać drogi sprzęt, taki jak generatory, ciągniki, koparki, wagony czy zbiorniki z paliwem i materiały podczas prac budowlanych. Wewnątrz budynków

mogą posłużyć do zabezpieczenia ścian, drzwi, sejfów, skarbców, bankomatów, szaf komunikacyjnych itp.

Działanie systemu V-Alert zostało przetestowane przez Izraelskie Laboratorium Testujące (ITL). Wyniki testów wykazały, że urządzenia spełniają wszystkie restrykcyjne wymagania dotyczące systemów tego typu. Sprawdzono m.in. kompatybilność elektromagnetyczną, klasy środowiskowe, a dodatkowo przebadano system w środowisku zagrożonym wybuchem. Producent deklaruje, że V-Alert spełnia wszystkie podstawowe wymagania europejskiej normy EN-50131-1:2009 w czwartym stopniu zabezpieczenia (*grade 4*).

Karta procesorowa jest urządzeniem wykonawczym, którego głównym zadaniem jest analiza sygnałów pochodzących z sensorów pracujących na liniach sensorowych. W zależności od tego, z jakimi urządzeniami karta będzie współpracować, informacje z niej możemy uzyskać na dwa sposoby. W najprostszym przypadku można wykorzystać wyjścia przekaźnikowe. W ten sposób każdą linię sensorową możemy podzielić na cztery strefy, a te z kolei przypisać do odpowiedniego wyjścia przekaźnikowego. Na karcie znajdują się również dwa wyjścia informujące o przecięciu lub innym uszkodzeniu linii sensorowej. Możemy zatem połączyć system V-Alert z dowolnym systemem alarmowym, modułem komunikacji GSM lub radiowym systemem powiadamiania.

Drugim sposobem uzyskania informacji z karty procesorowej jest wykorzystanie złącza RS232 i protokołów komunikacyjnych. W ten sposób można uzyskać informację o naruszeniu linii sensorowej z dokładnością co do sensora. Obecnie możemy połączyć system V-Alert z oprogramowaniem do integracji systemów zabezpieczeń VENO oraz z oferowanymi przez producenta modułami. Urządzenia te służą do przesyłania danych na większą odległość, przechowywania danych w rejestrze oraz do nadzorowania pracy systemu za pomocą konsoli lub specjalistycznego oprogramowania.

System V-Alert wyróżnia się przede wszystkim wielofunkcyjnością sensorów, możliwością regulacji czułości każdego sensora z osobna oraz możliwością cyfrowej transmisji i analizy sygnałów. Ponadto cechuje się wysoką jakością wykonania elementów, bezawaryjnością pracy

Fot. 2. Sensor VAF3 zainstalowany na ogrodzeniu

Fot. 3. Przykład instalacji sensorów VAF3 na ogrodzeniu panelowym

Fot. 4. Przykład zabezpieczenia płotu na granicy Izraela z Egiptem

i niezawodnością. Może zostać w szerokim zakresie zintegrowany z innymi systemami i (lub) aplikacjami. Umożliwia precyzyjne wskazanie miejsca naruszenia chronionej strefy, dzięki czemu zwiększa bezpieczeństwo chronionego obiektu.

Bartłomiej Kwiatkowski
AAT HOLDING

AST DO BRAM DRZWI OKIEN

AST GWARANCJĄ DYSKRETNEJ OCHRONY OBIEKTU

SZEROKA GAMA UNIWERSALNYCH CZUJEK MAGNETYCZNYCH SKUTECZNE ZABEZPIECZENIE BRAM, DRZWI I OKIEN

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Rozwijamy się dzięki zaufaniu

Przodujący producent urządzeń i oprogramowania do systemów nadzoru wizyjnego zmienił nazwę (wcześniej Samsung Techwin, teraz Hanwha Techwin) i znak towarowy swoich produktów (WiseNet). Firma została wcielona do grupy kapitałowej Hanwha Group. Bob (H.Y.) Hwang PhD – Managing Director Europe w firmie Hanwha Techwin – powiedział nam, co jeszcze zmieni się po ogłoszeniu decyzji Hanwha Group o dalszym inwestowaniu w dział zabezpieczeń elektronicznych

Jaką strategią kierujecie się teraz, by osiągnąć swoje cele?

Nasza korporacja wspiera budowę zespołu Hanwha Techwin. Pomoc ta pozwoliła nam zainwestować w zaawansowany program rozwoju produktów, który jeszcze mocniej ugruntował naszą pozycję na rynku wizyjnych systemów dozorowych. Obecna oferta umożliwia projektantom optymalne dobieranie produktów przy tworzeniu różnych rodzajów systemów. Obecne badania i program dalszego rozwoju produktów bazują na współpracy z wybranymi partnerami technologicznymi, która ma zapewnić nam długoterminowy sukces.

Waszą ostatnią inicjatywą marketingową jest hasło „Rozwijamy się dzięki zaufaniu". Co dokładnie ono znaczy?

To hasło jest pewnego rodzaju przyrzeczeniem. Wyraża ono chęć długofalowej współpracy oraz zobowiązanie do ciągłego rozwoju naszych urządzeń. Chcemy iść naprzód z pasją i zaangażowaniem oraz wspierać użytkowników naszego sprzętu. Nasza determinacja w budowaniu zaufania do obecnego modelu dystrybucji i partnerów technologicznych przejawia się w wielu aspektach naszej działalności biznesowej. Szanujemy i doceniamy wiedzę i doświadczenie partnerów biznesowych na wszystkich etapach współpracy – od realizacji dostaw naszych produktów do wspólnego tworzenia zintegrowanych rozwiązań. Użytkownicy sprzętu mogą polegać na naszych rozwiązaniach, które podnoszą poziom bezpieczeństwa osób, budynków i majątku oraz poprawiają wydajność działań biznesowych.

Co możesz jeszcze powiedzieć o zaplanowanych działaniach firmy?

W dalszym ciągu będziemy dostarczać produkty konstruowane i produkowane przez te same zespoły ludzi i fabryki – jak dotychczas. Będziemy nieustannie pracować nad tym, aby kamery WiseNet, rejestratory wizyjne i oprogramowanie były zabezpieczone przed cyberatakami. Wprawdzie żaden producent nie może zapewnić, że jego urządzenia są w 100% odporne na ataki hakerskie, ale my mamy wdrożony program nieustannych testów i monitorowania zagrożeń, który pozwala na ich szybkie identyfikowanie. Postanowiliśmy, że będziemy otwarcie komunikować się z naszymi klientami, gdy pojawią się nowe zagrożenia, i szybko przygotowywać poprawione wersje oprogramowania układowego, aby je zwalczać.

Mocno podkreślacie znaczenie partnerstwa technologicznego z wieloma innymi producentami. Jaką korzyść przyniesie ono klientom?

Jesteśmy dumni ze sposobu, w jaki konstruujemy i produkujemy innowacyjne kamery i rejestratory, ale bierzemy pod uwagę również to, że nasi klienci chcą otrzymywać kompletne rozwiązania. Otwarta platforma programowa i duża moc obliczeniowa procesorów stosowanych w naszych kamerach WiseNet umożliwia uruchomienie wielu aplikacji analizujących treść obrazu. Mimo iż teoretycznie możemy uruchomić w kamerze dowolną aplikację, dokładnie sprawdziliśmy oprogramowanie przygotowane przez naszych partnerów technologicznych i przygotowaliśmy modele kamer z fabrycznie zainstalowanymi aplikacjami.

Dostępne są rozwiązania przystosowane do handlu detalicznego – kamery WiseNet z funkcjami zliczania osób i generacji map ciepła. Kamery te są gotowe do pracy zaraz po wyjęciu z pudełka. Mogą być źródłem informacji dotyczących zachowania klientów w sklepach i efektywności pracy sprzedawców, a także umożliwić ustalenie okresów najintensywniejszej sprzedaży. Dzięki temu możliwa jest optymalizacja procesu obsługi klientów. Wymienione rozwiązania zostały przygotowane z naszym partnerem technologicznym Facit Data Systems.

Oferujemy też rozwiązanie przeznaczone do wykorzystania w systemie służącym do nadzorowania ruchu drogowego i informowania o wypadkach. Powstało ono w wyniku współpracy technologicznej ze Sprinx Technologies. Nasze kamery WiseNet X zostały zintegrowane z systemem automatycznej detekcji wypadków w ruchu drogowym (AID – Automatic Incident Detection) sprzedawanym przez Sprinx Technologies. Kompletne rozwiązanie AID umożliwia automatyczną detekcję wypadków i innych niebezpiecznych zdarzeń na drogach, autostradach, w tunelach czy na skrzyżowaniach. System ten pracuje już w kilku tunelach w Wielkiej Brytanii i jest bardzo efektywny.

Oferujemy też rozwiązanie powstałe w wyniku współpracy z ekspertami w dziedzinie analizy treści obrazu z firmy FF Group, które umożliwia automatyczne rozpoznawanie tablic rejestracyjnych i ułatwia zarządzanie ruchem na parkingach.

Wspólnie z firmą NVIDIA będziemy pracować nad inteligentną platformą do analizy treści obrazu, wykorzystując jednostki graficzne tej firmy z funkcją Deep Learning. Dzięki temu będziemy mogli zastosować dodatkowe funkcje wykorzystujące sztuczną inteligencję. Kamery będą zdolne do podejmowania samodzielnych decyzji w niebezpiecznych sytuacjach. Będzie można wykorzystać je w miejskich systemach monitorowania, w handlu detalicznym i w nadzorze nad ruchem drogowym.

Ostatnio mocno promujecie nowe kamery z serii WiseNet X. Co je wyróżnia?

Gdy na początku tego roku wprowadziliśmy do sprzedaży kamery z serii WiseNet X, chcieliśmy, by wyznaczyły one nowy standard sieciowych kamer przemysłowych IP. Procesor WiseNet V jest zastosowany we wszystkich kamerach z nowej serii X o rozdzielczościach 2 Mpx i 5 Mpx. Jest to najwydajniejszy procesor, jaki kiedykolwiek zastosowano w kamerach przemysłowych. Umożliwia on trzy razy szybsze przetwarzanie danych niż w poprzednich modelach, dzięki czemu możliwe jest wydajne działanie aplikacji analizujących treść obrazu. Kamery z serii WiseNet X są wyposażone w bardzo skuteczny system WDR zapewniający dynamikę obrazu dochodzącą do 150 dB. Seria X to kamery do zadań specjalnych. Mają one podwójne gniazdo dla kart SD, co umożliwia autonomiczny zapis obrazu przez 24 godziny w pamięci o pojemności 512 GB. Jeśli połączenie sieciowe z rejestratorem ulegnie przerwaniu, kamera zapisze materiał wizyjny na karcie SD, a później, po ponownym uzyskaniu połączenia, przeniesie go do archiwum w rejestratorze.

Czy kamery WiseNet X staną się jeszcze bardziej popularne?

Z pewnością. Właśnie ogłosiliśmy, że przyspieszamy proces integracji kamer WiseNet X z Genetec Security Center 5.6 i Milestone XProtect oraz innymi popularnymi aplikacjami VMS. To kolejny przykład rozwijania się dzięki zaufaniu. Współpracujemy z partnerami technologicznymi, ponieważ chcemy, aby użytkownicy naszych urządzeń byli zadowoleni z ich użytkowania i aby mogli czerpać coraz nowsze korzyści ze stosowania systemów nadzoru wizyjnego.

EXTREMALNA WYDAJNOŚĆ

WISENET X

- Zobacz najlepszą na świecie funkcję WDR 150 dB
- 4 różne prędkości migawki dla stworzenia jednego, bardziej naturalnego obrazu
- Wyjątkowa czytelność z regulowanymi poziomami jasności nawet przy oślepiającym świetle

WORLD BEST

Odkryj więcej na www.WisenetX.com

Hanwha Techwin

ZARZĄDZANIE BEZPIECZEŃSTWEM

Nowe rozwiązania*

100 dni w biurze Fokko van der Zeego

Zdaje się, że Nedap Security Management załatwia sprawy inaczej: Można odnieść wrażenie, że programiści siedzą przy jednym biurku z pracownikami obsługi klienta. I dokładnie w to celuje holenderskie przedsiębiorstwo: Rozwijanie produktów dostosowanych do klientów. Niedawno Nedap Security Management przyjęło nową osobę na wiodącą rolę: Fokko van der Zee jest nowym Dyrektorem Zarządzającym przedsiębiorstwa. Po ogłoszeniu tej wiadomości na IFSEC, Lisa Schneiderheinze z GIT SECURITY miała możliwość uściśnięcia jego dłoni i po jego trzech miesiącach na stanowisku udało jej się z nim porozmawiać na temat Nedap i branży.

GIT SECURITY: Marynarka, służba zdrowia, a teraz bezpieczeństwo! Przebył Pan długą drogę. Czy istnieje jakiś połączenie z Pańskim wcześniejszym doświadczeniem zawodowym?

Fokko van der Zee: Tak, można powiedzieć, że istnieje takie połączenie. We wszystkich branżach, w których działałem, istotna była zaawansowana technologia, ale też potrzeba balansowania technicznej złożoności i udziału człowieka. Oprócz tego na wszystkich moich stanowiskach ważny był duch współpracy. Lubię współpracować z ludźmi i mieć do czynienia z technologią i innowacjami. Myślę, że podświadomie zawsze poszukiwałem takiego połączenia w stanowiskach, które wybierałem. Dokładnie z takim połączeniem zaawansowanej technologii i czynnika ludzkiego mam do czynienia na moim obecnym stanowisku w Nedap. A Nedap jest zdecydowanie innowacyjny – cały czas szukamy nowych, bardziej skutecznych sposobów mierzenia się z wyzwaniami.

Co w branży bezpieczeństwa wzbudziło Pańskie zainteresowanie?

Fokko van der Zee: Ze względu na moje zainteresowanie technologią, miałem Nedap na uwadze – to uznany lider w dziedzinie technologii, który jest skupiony na przedsiębiorczości i ciągłym rozwoju. Bycie częścią takiej organizacji naprawdę przyciągnęło moją uwagę. Dzisiejszy świat jest płynny, wrażliwy i szybko się zmienia. Mierzymy się nie tylko z fizycznymi zagrożeniami, ale przez prędkość zmian w technologii również z cyber-atakami. Chcę przyczynić się do rozwiązywania tych poważnych problemów i sprawić, by każdy mógł korzystać z życia w bezpiecznym świecie. Odpowiadanie na potrzeby współczesnego społeczeństwa i działanie na jego rzecz to moja siła napędowa. Wierzę, że dołączenie do branży bezpieczeństwa, w szczególności w tak postępowej organizacji jak Nedap, sprawi, że będę mógł to robić.

"Kontrola dostępu jest w centrum naszych zainteresowań i doskonale rozumiemy modele autoryzacji.".

Spędził Pan już 100 dni na stanowisku – gratulacje! Co najbardziej Pana zaskoczyło w Nedap?

Fokko van der Zee: Wiele przedsiębiorstw mówi o docenianiu swoich pracowników i tym, że to ludzie stoją za postępem, ale w przypadku Nedap jest to prawda. To nie są słowa bez pokrycia – Nedap inwestuje w tworzenie najlepszego możliwego środowiska pracy i pomaganie pracownikom w rozwijaniu się. W istocie, pomimo tego, że Nedap to przedsiębiorstwo zajmujące się technologią, jedną z jego kluczowych wartości jest docenianie wkładu ludzi w postęp. Płaska struktura organizacyjna w Nedap to również nietypowe podejście, które jest kluczem do sukcesu. Oznacza to, że oprócz wspierania indywidualnej przedsiębiorczości i innowacji, każdy ma prawo i wolność myślenia poza szablonami. W połączeniu z uwagą poświęcaną rekrutowaniu i rozwijaniu na wysokim poziomie wiedzy fachowej tworzy to silny zespół.

Bazując na Pańskim wcześniejszym doświadczeniu, co planuje Pan zmienić w Nedap Security Management w przyszłości?

Fokko van der Zee: Nedap to wyjątkowa organizacja i jej siła tkwi w jej oryginalności. Nie znaczy to więc, że chciałbym coś zmienić, raczej chcę się skupić na rozwijaniu naszych mocnych stron. Oczywiście ze względu na to, że żyjemy w szybko zmieniającym się świecie, w przyszłości będzie istotne, abyśmy pozostali elastyczni i szukali nowych sposobów, aby móc się jeszcze lepiej przystosowywać.

Nedap zapewnia, że oferuje klientom spersonalizowane rozwiązania, a nie gotowe systemy. Oferowanie rozwiązań klientom to wspaniała misja, ale czasami trudno wyobrazić sobie, czym zajmuje się Pańskie przedsiębiorstwo. Czy mógłby Pan opisać ofertę Nedap Security Management w kilku zdaniach?

Fokko van der Zee: Zdajemy sobie sprawę z tego, że czasami jest trudno zrozumieć wszystko, czym się zajmujemy. Kontrola dostępu jest w centrum naszych zainteresowań i doskonale rozumiemy modele autoryzacji. Oferujemy zarówno oprogramowanie jak i sprzęt do zarządzania fizycznymi zabezpieczeniami. Oprócz tego, wierzymy, że fizyczne zabezpieczenia powinny być chronione przed wszystkimi rodzajami włamań we współczesnym świecie. Dlatego też opracowaliśmy system bezpieczeństwa "end-to-end", który gwarantuje szyfrowanie połączeń między kartą, kontrolerem i serwerem. Ogółem chcemy umożliwić naszym partnerom dystrybucyjnym spełnianie wymagań klientów systemów zarządzania bezpieczeństwem. Nasz produkt, AEOS, można swobodnie konfigurować, więc nasi partnerzy dystrybucyjni mogą tworzyć systemy odpowiadające konkretnym potrzebom klientów i zgodne z przepisami miejscowymi.

System zarządzania bezpieczeństwem AEOS łączy w sobie kontrolę dostępu, zarządzanie video i wykrywanie włamań na jednej platformie. Jednak rynek cały czas się zmienia. Jak zapewni Pan, że system będzie się sprawdzać w przyszłości?

Fokko van der Zee: Ze względu na to, że branża kontroli dostępu ciągle się zmienia, musimy stale inwestować w rozwijanie i poprawianie AEOSa. Otwartość AEOSa jest dla nas ważna. Skupiamy się na rozwoju API, co pozwala na optymalne połączenie z systemami innych producentów. Poprzez wykorzystywanie naszych API i standardów branżowych, możemy zwiększyć możliwości integracji z czołowymi partnerami w branży technologicznej. Aby uzyskać szczegółowy know-how w dziedzinach pokrewnych do kontroli dostępu, również integrujemy się z rozwiązaniami najlepszymi w swojej klasie, takimi jak produkty Milestone, przedsiębiorstwa, z którym nawiązaliśmy współpracę w zakresie integracji video. Wierzę, że te dwa aspekty, połączone z ogromną elastycznością AEOSa i nasze ciągłe śledzenie bieżących i przyszłych potrzeb, sprawią, że będziemy przygotowani na przyszłość.

"Nedap to przedsiębiorstwo skoncentrowane na rozwoju, a zmiany dają nam mnóstwo możliwości do rozwijania się. Powiedziałbym, że opieramy się na tym.".

Czy ciągłe zmiany w technologii to przekleństwo czy błogosławieństwo i dlaczego?

Fokko van der Zee: Wydaje mi się, że to ani jedno, ani drugie – to po prostu fakt, który musimy mieć na uwadze. Nedap to przedsiębiorstwo skoncentrowane na rozwoju, a zmiany dają nam mnóstwo możliwości do rozwijania się. Powiedziałbym, że opieramy się na tym.

Nedap twierdzi, że AEOS jest bardziej elastyczny i łatwiejszy w obsłudze niż inne systemy bezpieczeństwa. Czy mógłby Pan udowodnić te stwierdzenie i podać przykłady?

Fokko van der Zee: Reszta rynku korzysta z kontrolerów, które mogą zajmować się tylko jednym zadaniem, a nasze kontrolery mogą robić wszystko, co klienci chcą, żeby robiły i mogą je modyfikować, kiedy chcą. Jest to możliwe dzięki rozdzieleniu sprzętu od oprogramowania – każdy z naszych kontrolerów ma wysoką zdolność przetwarzania, więc oprogramowanie może określać ich zastosowanie.

Dziękujemy!

Bezpieczeństwo informacji a infobrokerstwo (część 1)

Broker informacji – jego rodowód i użyteczność zawodowa

dr inż. Marek Blim

> Przedsiębiorca odczuwający potrzebę uzupełnienia zasobu posiadanych informacji o rynku i działaniu na nim innych firm z branży na pewno zainteresuje się pozyskaniem jej w sposób legalny. Wówczas może skorzystać z usług odpowiedniego specjalisty

Obecnie dostępny jest ujednolicony tekst załącznika do rozporządzenia Ministra Pracy i Polityki Społecznej z 27 kwietnia 2010 r. (Dz. U. z 2010 r, Nr 82, poz. 537 z późniejszymi zmianami – Dz. U. z 2012 r, poz. 1268). Jest to klasyfikacja zawodów i specjalności, w której pod numerem 262204 wymieniony jest broker informacji (researcher). Jest też Polska Klasyfikacja Działalności z 2007 r., w której wymieniony jest rodzaj działalności określany jako „pozostała działalność usługowa w zakresie informacji, gdzie indziej niesklasyfikowana" (63.99.Z). Należy jednak wyjaśnić, co właściwie kryje się pod tymi określeniami.

Infobrokerstwo, infobroker i jego działalność

Słowo *infobrokerstwo* jest kolejnym spolszczeniem funkcjonującego od dwudziestu lat w bibliotekoznawstwie polskim słowa *infobrokering* określającego komercyjne, zawodowe pośrednictwo (mediację) w świecie informacji. Człowiek parający się tym zajęciem bywa nazywany różnie (choć niekoniecznie w pełni poprawnie) – brokerem informacji, infobrokerem, researcherem, specjalistą od informacji (co koresponduje z określeniami zagranicznymi: angielskim *information professional* lub niemieckim *infobroker*). Zbitka językowa *infobroker* w pełni opisuje i oddaje sens jego działań zawodowych jako osoby, która pośredniczy (stąd *broker*) pomiędzy zasobem informacyjnym (stąd *info*) a klientem zlecającym mu specjalistyczne opracowanie.

Infobroker jest więc specjalistą w zakresie zbierania informacji i zarządzania nimi bądź prowadzącym własną działalność gospodarczą (*independent information professional*), bądź też pracownikiem etatowym firmy zajmującej się przetwarzaniem informacji (jako broker innowacji lub technologii) lub doraźnym (jako freelancer) realizatorem projektów informacyjnych. Infobroker nie sprzedaje informacji, tylko usługę, która może polegać na sporządzeniu opracowania, raportu czy bazy danych.

Historia infobrokerstwa na świecie i w Polsce

Prywatyzowanie w USA zasobów bibliotekarskich w latach 60. i 70. XX wieku przyczyniło się bezpośrednio do powstania w 1987 roku stowarzyszenia The Association of Independent Information Professionals (AIIP) będącego źródłem informacji dla przedsiębiorców, dzięki któremu każdy zainteresowany właściciel firmy mógł uzyskać potrzebną mu informację w oczekiwanej zrozumiałej postaci i w dostosowanym do jego potrzeb zakresie. Głównymi zadaniami AIIP były i nadal są:

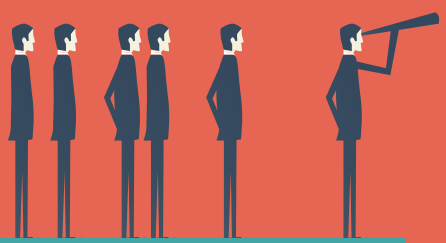
– szerzenie wiedzy na temat zawodu infobrokera,
– stworzenie i wprowadzenie w życie etycznych standardów prowadzenia tego typu działalności,
– zachęcenie niezależnych infobrokerów do prowadzenia dyskusji na wspólne tematy,
– promowanie wymiany informacji pomiędzy infobrokerami,
– informowanie społeczeństwa o istnieniu i sposobach działania brokerów informacji.

Obecnie AIIP skupia około 700 członków na całym świecie i choć stowarzyszenie nie ma swego oddziału w Polsce, to od lat kodeks etyczny AIIP jest powszechnie stosowany w naszych firmach infobrokerskich. Użytkową odmianą biznesową infobrokerstwa zajmuje się od 1989 roku amerykańska sieć Strategic and Competitive Intelligence Professionals (SCIP) mająca od ponad dziesięciu lat swój polski oddział.

Charakterystyczne jest to, że w amerykańskiej nomenklaturze i nazewnictwie zawodowym nie występują nazwy *infobrokering* i *infobroker*, co wynika z nie zawsze pozytywnych skojarzeń, które budzi słowo *broker*.

O brokerstwie informacyjnym w Polsce możemy mówić w kilku różnych aspektach:

– edukacyjnym (w Instytucie Informacji Naukowej i Bibliotekoznawstwa UJ od 1993 r. prowadzony jest przedmiot informacja biznesowa);
– teoretycznym (wystąpienie Katarzyny Materskiej, obecnej prof. bibliologii UJ, w 1997 roku na 6. międzynarodowym seminarium *Scientific and Technical Information in Central and Eastern Europe* z referatem pt. *Broker informacyjny i jego rola w rozwoju nauki*);
– praktycznym (założenie w 1999 roku przez Piotra Kamińskiego firmy Fabryka Informacji oferującej jako agencja infobrokerska usługi z zakresu monitorowania prasy, opracowywania raportów oraz śledzenia informacji w materiałach informacyjnych);



– rynkowym (absolwenci studiów na UJ w Krakowie i UMK w Toruniu oraz uczestnicy kursów CPI w Warszawie zaczęli zakładać w latach 2003–2005 kolejne firmy *stricte* infobrokerskie, natomiast już wcześniej istniejące firmy oferujące usługi informacyjne wprowadziły elementy researchu oferowane klientom biznesowym i projektowym. W okresie do 2010 roku zaistniało na polskim rynku około 70 firm infobrokerskich. Obecnie usługi tego typu oferuje 17, 24 lub 38 firm, a jako zgłoszone w korelacji z innymi działaniami informacyjnymi oferowane są przez ok. 220 przedsiębiorstw z branży IT lub I&CT. Usługi zbliżone, cząstkowe lub mieszane oferowało na koniec 2015 roku ponad 700 firm lub osób.

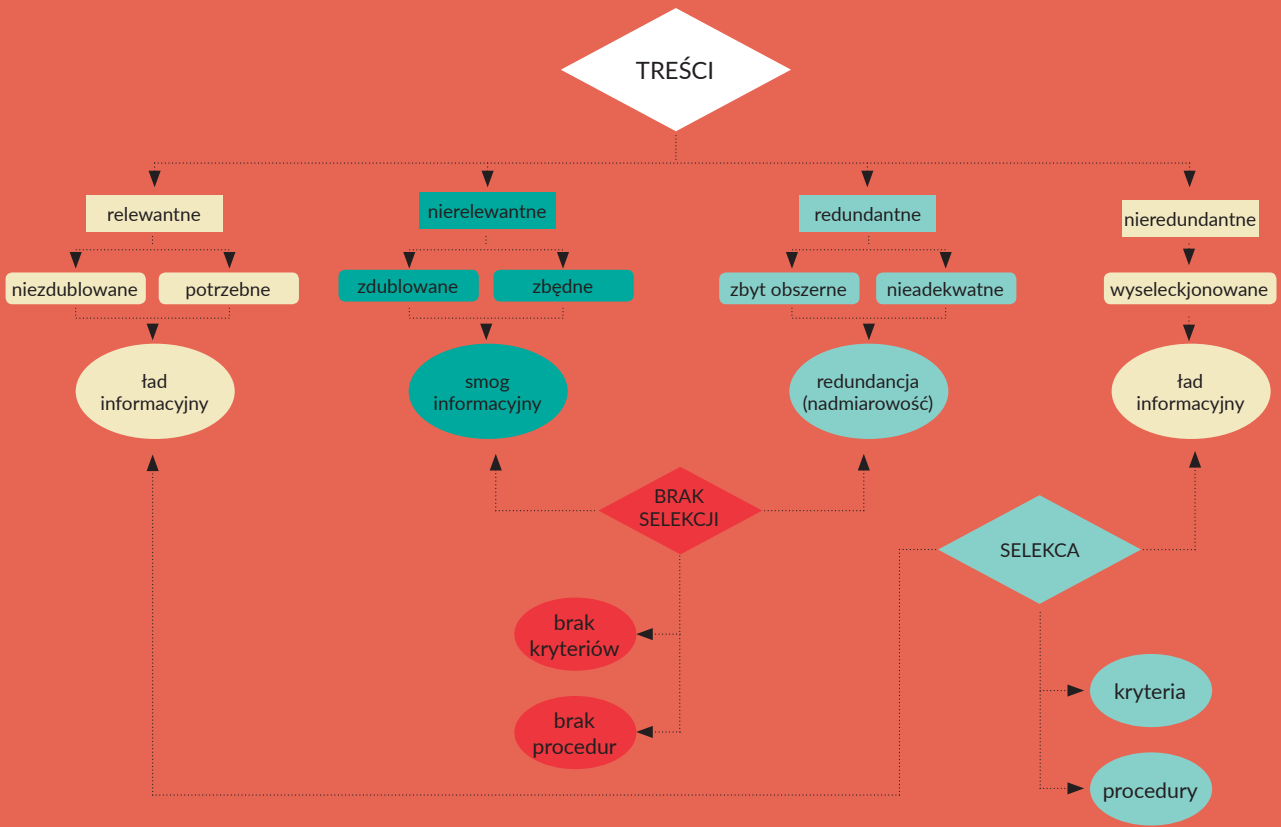
Międzynarodowe źródła informacji – ich dostępność oraz użytkowość

Do podstawowych atrybutów informacji mogą należeć:
– poufność – rozumiana bardzo szeroko (od informacji niejawnej, przez nieujawnione tajemnice handlowe i zawodowe, aż po informacje osobowe, wrażliwe, medyczne i in.;
– integralność – rozumiana głównie jako spójność wewnętrzna (np. spójność informacji w komunikacie, pliku, rekordzie w bazie danych);
– dostępność – odnosząca się w tym przypadku nie do jej ograniczania (zasoby niejawne i nieujawnione), lecz do łatwości dostępu i odczytania przy jednoczesnym (mocno ograniczonym) prawie do wprowadzania ew. zmian formalnych i aktualizacji.

Normatywne podejście do informacji (formalizacja) odbiega w sposób znaczący od cech, jakich oczekuje się w działaniach między klientem a infobrokerem, kiedy to za najważniejsze w dobrej informacji uznaje się jej:
– użyteczność – informacja musi treściowo odpowiadać pewnej potrzebie, na ogół związanej z podjęciem pewnej decyzji;
– dostępność – informacja musi być osiągalna dla zainteresowanej osoby, co oznacza, że musi być w miarę tania i rozpowszechniana w kręgu właściwych użytkowników;
– operatywność – informacja musi być aktualna, uzyskana na czas, na ogół szybko;
– trafność – informacja musi być adekwatna, tzn. trafiać w sedno, dotyczyć danej kwestii, nie pomijając istotnych elementów;
– zrozumiałość – informacja musi być podana we właściwym języku, być przystępna i identyfikowalna;
– prawdziwość – informacja musi przedstawiać sprawy tak, jak mają się one w rzeczywistości, nazwać rzeczy po imieniu;
– wiarygodność – informacje muszą pochodzić z wiarygodnego źródła;
– rzetelność – informacja musi przedstawiać dokładnie i starannie;
– weryfikalność – informacja powinna być możliwa do sprawdzenia, uzupełnienia oraz rozszerzenia.

Wszystkie te cechy można przypisać informacjom organizacji międzynarodowych i międzypaństwowych. Są wiarygodne (wytworzone przez oficjalne podmioty) i zarazem dostępne online nieodpłatnie dla wszystkich zainteresowanych. Warto pamiętać, że zbiory tych informacji są ogromne i że dotyczą one wielu aspektów i dziedzin – jeżeli tylko potrafimy, to znajdziemy wiele przydatnych informacji różnego typu. Przykładami niech będą zasoby z dziedzin edukacji, nauki i techniki lokowane pod różnymi adresami, np. w OECD Science, Technology and R&D Statistics (http://www.oecd-ilibrary.org/science-and-technology/data/oecd-science-technology-and-r-d-statistics_strd-data-en), a także analizy, prognozy czy raporty, np. WTO World Trade Report 2016 (https://www.wto.org/english/res_e/publications_e/wtr16_e.htm).

Z myślą o poprawności informacyjnej brokera warto przypomnieć anegdotyczne pytanie zadane gwieździe warszawskiej palestry: „Czy to prawda, że zna pan, panie mecenasie, całe prawo karne wraz z glosariuszem?", a także lekko ironiczną



Rys. 1. Podstawowe błędy w analizie treści wymaganych od infobrokera. Przyjrzyjmy się uważnie zakresowi oczekiwanych kompetencji

odpowiedź: „Co do prawa, to sądzę, że dość dobrze poznałem wszystkie jego luki i nieścisłości. O glosariuszu nie będę się tu i teraz wypowiadał".

Zróżnicowane postrzeganie infobrokerstwa w Polsce

Charakterystycznymi cechami rynku usług infobrokerskich w Polsce są heterogeniczność, niematerialność, nietrwałość, jednoczesność świadczenia i korzystania z usług oraz przenikalność kompetencji. Wszystkie podmioty działające na tym rynku zajmują się zawodowym, profesjonalnym wyszukiwaniem, pozyskiwaniem, analizowaniem, ocenianiem i dostarczaniem informacji. Heterogeniczność rynku polega na trudności standaryzacji usług infobrokerskich, gdyż jest ich wiele, a każda firma dostosowuje je do potrzeb swego odbiorcy. *„Nie jest możliwe ujednolicenie usług, skierowanych dla spełnienia potrzeb informacyjnych indywidualnych klientów. Nawet jeśli zlecenia dotyczą podobnego obszaru, na przykład kontaktów do hurtowni perfum. Dla każdego klienta ważne są inne parametry i warunki, jakie powinna spełniać poszukiwana hurtownia. Dla jednego ważna jest cena perfum, dla innego zaś sposób składania zamówienia. Usług nie da się zapakować do pudełka i postawić na półce w sklepie. Sprzedaż usług jest sprzedawaniem czegoś niewidzialnego"*[1] .

Analizy polskiego rynku infobrokerskiego dotyczące okresu ostatniego dziesięciolecia, przeprowadzane pod kątem użyteczności i skuteczności usług infobrokerskich, odwołują się często do krajowego standardu kompetencji zawodowych brokera informacji. Standard ten został opracowany i opublikowany w 2013 r. Znaczenie unormowania działania brokera wynika przede wszystkim z konieczności uściślania informacji dla klienta (rys. 1.).

Perspektywy rozwoju branży infobrokerskiej

Powstająca w Polsce branża usług informacyjnych wytyczyła w krótkim czasie trzy różne drogi dalszego rozwoju. Stały się nimi:

- infobrokerstwo jako działalność własna podmiotów gospodarczych lub tzw. freelancerów, włączanych doraźnie do projektów informacyjnych, o zróżnicowanym poziomie wiedzy i praktyki;
- określana mianem brokerstwa systemowego wewnętrznego działalność informacyjna ukierunkowana na potrzeby własne organizacji, głównie występująca w dużych firmach lub korporacjach i mająca charakter brokerstwa

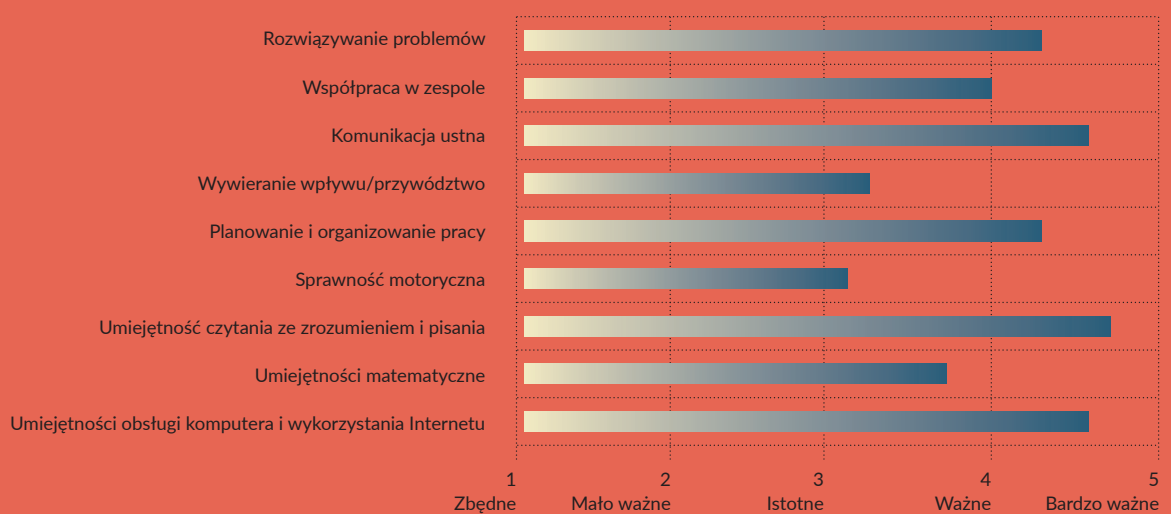
[1] Cisek S., „Broker informacji w społeczeństwie wiedzy: istota zawodu", mat. konf. IINiB UJ, Kraków 2008.

innowacyjnego lub technologicznego;
– działalność szeroko rozumianych wywiadowni gospodarczych (o ich działaniach będzie kilka słów w kolejnym podrozdziale).

Zakres działań brokera informacji (infobrokera) możemy zamknąć w „dekalogu":

1. Wyszukiwanie informacji istotnych w odniesieniu do zapytania klienta.
2. Dobieranie metody realizacji zlecenia (rozpoznawanie potrzeb informacyjnych, budowanie strategii wyszukiwania i dobierania źródeł).
3. Ocenianie jakości źródeł informacji i selekcja informacji.
4. Analizowanie źródeł z zastosowaniem metodologii dziedzinowych.
5. Prowadzenie dokumentacji dotyczącej realizacji zlecenia.
6. Tworzenie raportów, baz danych i innych opracowań infobrokerskich.
7. Monitorowanie źródeł informacji i aktualizacja zasobów informacyjnych.
8. Przestrzeganie obowiązujących procedur, przepisów, norm oraz zasad poufności informacji.
9. Organizowanie stanowiska pracy zgodnie z zasadami i przepisami BHP, ochrony ppoż., ergonomii i ochrony środowiska.
10. Zaakceptowanie faktu, że broker informacji to wyodrębniony zawód, który może być wykonywany przez każdego, kto posiada odpowiednie kompetencje i umiejętności.

Oczywiście nie zapominajmy o wymaganych kompetencjach zawodowych:



Rys. 2. Kluczowe kompetencje dla zawodu nr 222604 (broker informacji – researcher)

Infobroker a inni specjaliści od informacji

Tematowi szczególnemu, a mianowicie związkom brokera technologii i innowacji z ochroną i bezpieczeństwem informacji nieujawnionej, ze względu na jego obszerność poświęcona będzie druga część artykułu, a kolejnemu wywiadowczemu kierunkowi rozwoju usług informacyjnych poświęcony jest ten podrozdział.

Będzie esencjonalnie i krótko. Dlaczego? Wywiadownie (głównie deklarujące się jako gospodarcze), niezależnie od składanych zapewnień i zobowiązań etycznych, w prowadzonych działaniach bardzo często kierują się tzw. moralnością Kalego lub własną (mocno wysublimowaną) etyką biznesową, pozwalającą im na znacznie więcej, niż może nam się wydawać. Ograniczę się zatem do kilku stwierdzeń odnoszących się do ofert wywiadowni w Polsce. Większość z nich:

– proponuje usługę wywiadu gospodarczego, oferując sprawdzanie podmiotów gospodarczych w zakresie podstawowym i rozszerzonym, na terenie kraju i poza jego granicami,
– zajmuje się gromadzeniem, analizą i dostarczaniem informacji o moralności płatniczej firm (czyli nagminnym stosowaniu kruczków prawnych odciągających terminy zapłaty faktur i rachunków – jest to forma okresowego finansowania działalności dłużnika z pieniędzy wierzycieli),
– gromadzi materiały obciążające (wobec obserwowanych firm/osób) oraz prowadzi windykację należności na rzecz zlecającego.

Szereg z nich oferuje rozwiązania z zakresu doradztwa gospodarczego i finansowego, udziela e-mailowych, odpłatnych porad dotyczących windykacji, oddłużania, wywiadu. Niektóre, będące filiami firm zagranicznych, umożliwiają dostęp online do raportów kredytowych o 50 mln publicznych oraz prywatnych przedsiębiorstw z wielu krajów świata. Nieliczne są wyspecjalizowane w pracach rozpoznawczych i ustaleniowych na terenie całego kraju oraz w reprezentowaniu poszkodowanych klientów w postępowaniu karnym. Zajmują się również wykrywaniem urządzeń podsłuchowych oraz bezpieczeństwem procesów inwestycyjnych (także transgranicznych).

Jak więc widać, sporo tutaj działań z zakresu infobrokerki, ale pozyskiwanie informacji gospodarczych i zarządzanie nimi w imieniu klientów ma już nieco inną wymowę.

Kiedy zatem spotkamy się z firmą, która w ramach usług infobrokerskich proponuje nie tylko usługi podstawowe (wyszukiwanie i pozyskiwanie informacji na zlecenie, tworzenie raportów i analiz, budowa baz danych), ale i dodatkowe (monitorowanie Internetu, mediów, konkurencji, newsów, weryfikacja danych, faktów, usługi tekstowe, zarządzanie informacją i wiedzą, marketing internetowy i bezpieczeństwo informacji), to przede wszystkim sprawdźmy, czy przypadkiem faktyczny zakres działalności i możliwości naszego oferenta nie jest jeszcze większy i czy służy on naszym celom i potrzebom.

Opracował dr inż. Marek Blim

Bibliografia

1. Beckwith H., *Sprzedawanie niewidzialnego. Przewodnik po nowoczesnym marketingu usług*, wyd. Helion, Gliwice 2006.
2. Hrabiec-Hojda P., *Specyfika usług infobrokerskich a kompetencje informacyjne infobrokera*, *„Bibliotheca Nostra”*, nr 1 (31)/2013, Katowice 2013.
3. *Krajowy standard kompetencji zawodowych. Broker informacji (researcher) (222604)*, wyd. Ministerstwo Pracy i Polityki Społecznej, Centrum Rozwoju Zasobów Ludzkich, Warszawa 2013.
4. Cisek S. (red.), Januszko-Szakiel A. (red.), *Zawód infobroker. Polski rynek informacji*, Wolters Kluwer, Warszawa 2015.
5. Małek A. (red.), Kamieniecka M. (red.), Jackowska U. (red.), *Brokerstwo systemowe – teoria i praktyka*, Lubelski Park Technologiczny, Lublin 2014.
6. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 27 kwietnia 2010 roku w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (Dz. U. z 2010 r., nr 82, poz. 537 z późn. zm.).
7. Ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (t.j.: Dz. U. z 2014 r., poz. 1015 z późn. zm.).

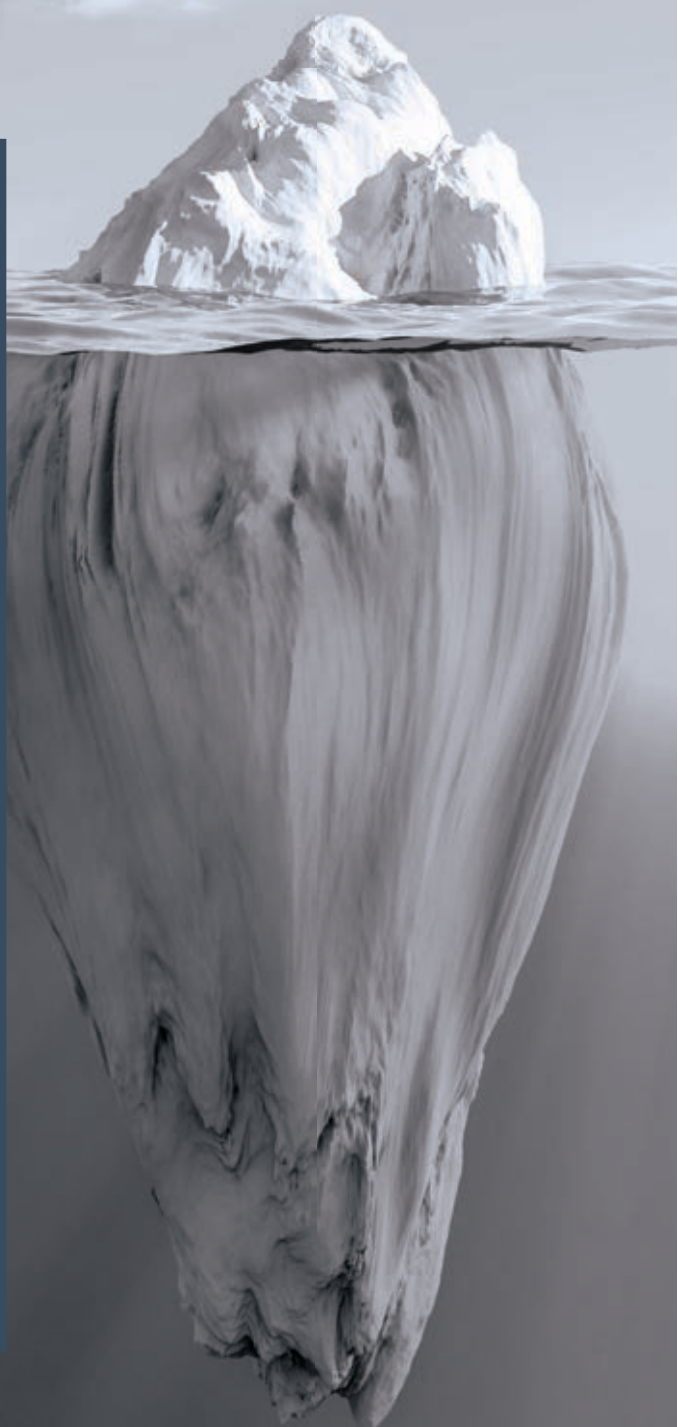
Prezentacje
https://prezi.com/-hezqz1th980/raport-o-rynku-firm-infobrokerskich/
https://prezi.com/-hezqz1th980/raport-o-rynku-firm-infobrokerskich/
https://www.slideshare.net/sabinacisek/afm-krakw-2015-cisek
https://www.slideshare.net/sabinacisek/organizacje-midzynarodowe-jako-niekomercyjni-dysponenci-informacji?next_slideshow=1
https://www.spi.org.pl/2017/02/06/warsztat-pracy-infobrokera-materialy-konferencyjne/

Materiały
http://katalog.wp.pl/infobrokerzy/
http://www.infobrokerka.pl
http://www.infobrokerstwo.pl
http://www.infoiprawo.blogspot.com
https://www.researchgate.net/publication/313820834_Infobrokering_i_wywiad_rynkowy_podstawy_16_17
http://www.sbc.org.pl/Content/72732/bn_1_2013.pdf

Przeprowadzanie audytu

dotyczącego zarządzania bezpieczeństwem organizacyjno-technicznym obiektów. Część 3 Szacowanie ryzyka w związku z ochroną informacji

dr inż. Andrzej Wójcik



W drugiej części artykułu (*Zabezpieczenia* nr 4/2017) omówione zostały wymagania dotyczące przeprowadzania audytu. Według wymienionych standardów normatywnych i biznesowych jedną z kluczowych metod oceny bezpieczeństwa organizacji jest szacowanie ryzyka. Można stwierdzić, że nieoszacowanie ryzyka jest naruszeniem fundamentalnych zasad bezpieczeństwa organizacji. Oszacowanie ryzyka powinno być udokumentowane, oparte na opracowanej i zatwierdzonej metodyce oraz dokonywane systematycznie i w określonych okolicznościach, np. w przypadku niebezpiecznego incydentu. Ważne są uzyskane wyniki, ich wpływ na wybór zabezpieczeń oraz sprawdzenie skuteczności tych zabezpieczeń. Organizacja szacuje ryzyko i określa zależny od wyników plan postępowania. To wszystko należy udokumentować oraz przedstawić audytorowi i zainteresowanym stronom w celu wykazania, że zarządzanie bezpieczeństwem w organizacji przebiega prawidłowo

Informacje na temat szacowania ryzyka zawarte w aktach prawnych i normach

Szacowania ryzyka w związku z ochroną informacji dotyczą niektóre akty prawne, np. ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228). W art. 2 rozdziału 1, w którym zawarte są przepisy ogólne, zdefiniowano szacowanie ryzyka. Zgodnie z zapisami w ustawie ryzyko jest kombinacją prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji, szacowania ryzyka jest całościowym procesem analizy i oceny ryzyka, a zarządzanie ryzykiem to skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji z uwzględnieniem ryzyka. Ustawowe definicje są zbliżone do określeń zawartych w normach zarządzania bezpieczeństwem informacji.

W art. 15 rozdziału 3 dotyczącego organizacji ochrony informacji niejawnych wskazano, kto jest odpowiedzialny za szacowanie ryzyka. Tą osobą jest tzw. pełnomocnik ochrony. Do zadań pełnomocnika należy także zarządzanie ryzykiem związanym z ochroną informacji niejawnych, w szczególności szacowanie ryzyka. Porównując zapis w art. 15 z wymaganiami zawartymi w normach dotyczących bezpieczeństwa informacji, można stwierdzić dużą zbieżność, ponieważ normy te wskazują właścicieli zasobów (aktywów) informacyjnych, tzw. właścicieli ryzyka, którzy są odpowiedzialni za proces szacowania ryzyka.

W dalszej części omawianej ustawy, w art. 19 rozdziału 4, omówione zostały zasady szkolenia mającego na celu zapoznanie się z „zasadami zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka", a także ze „sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia". Szkolenie w zakresie szacowania ryzyka oraz zrozumienie tego procesu jest narzucone także w zapisach normatywnych dotyczących zarządzania bezpieczeństwem informacji.

Na zakończenie rozważań o ustawie przytaczam zapisy z art. 43 rozdziału 7 dotyczącego środków bezpieczeństwa fizycznego w kancelariach tajnych: „Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne o klauzuli «poufne» lub wyższej, zatwierdza opracowaną przez pełnomocnika ochrony dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą".

Cytowana ustawa była pierwszym tak bardzo szczegółowo opisującym proces zarządzania ryzykiem aktem prawnym. Oczywiście w aktach wykonawczych opisano szczegółowe wymagania dotyczące szacowania ryzyka i postępowanie z ryzykiem w systemach IT przetwarzających informacje niejawne. Te wymagania zostały zawarte w rozporządzeniu Prezesa Rady Ministrów z 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948). Rozporządzenie definiuje zarządzanie ryzykiem i plan postępowania z ryzykiem w przypadku systemu teleinformatycznego przetwarzającego informacje niejawne poprzez realizację procesów:
– szacowania ryzyka dotyczącego bezpieczeństwa informacji niejawnych;
– postępowania z ryzykiem;
– akceptacji ryzyka;
– przeglądu, monitorowania i informowania o ryzyku.

Zgodnie z rozporządzeniem przed oszacowaniem ryzyka wykonuje się następujące czynności:
– ustala się granice i zakres analizy ryzyka;
– ustanawia się strukturę organizacyjną odpowiedzialną za zarządzanie ryzykiem w systemie teleinformatycznym;
– dokonuje się wyboru metody analizy ryzyka.

Kończąc rozważania dotyczące ochrony informacji niejawnych, należy wspomnieć o rozporządzeniu Rady Ministrów z 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012 r., poz. 683). Określono w nim:
– podstawowe kryteria i sposób określania poziomu zagrożeń;
– dobór środków bezpieczeństwa fizycznego dostosowanych do wskazanego poziomu zagrożeń;
– rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomów zagrożeń;
– podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;
– zakres stosowania środków bezpieczeństwa fizycznego;
– kryteria tworzenia stref ochronnych.

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych zawiera odwołania do szczegółowych wymagań normatywnych, w tym wymagań odnoszących się do szacowania ryzyka oraz do norm z zakresu bezpieczeństwa informacji, tj.:

I. Wymagane jest zapewnienie „okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok".
II. System zarządzania bezpieczeństwem informacji powinien być opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a „ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, tj.:
1. PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;
2. PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
3. PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania".

Należy dodać, że norma PN-ISO/IEC 17799 została wycofana i zastąpiona przez normę PN-EN ISO/IEC 27002:2017-06 *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji*.

W maju 2018 r. wejdzie w życie RODO, które spowoduje rewolucję w dziedzinie przetwarzania danych osobowych. Rozporządzenie to wprowadza szereg obowiązków dla administratorów danych. Chodzi o konieczność oceny ochrony danych osobowych już na etapie projektowania rozwiązań (*privacy by design*), konieczność przeprowadzenia analizy ryzyka utraty prywatności (*privacy impact assessment*) oraz stworzenie planu reakcji na niebezpieczny incydent (*breach response plan*).

Normatywne podstawy szacowania ryzyka

Celem usystematyzowania i przypomnienia warto podać normy regulujące szacowanie ryzyka w systemach zarządzania bezpieczeństwem informacji, m.in. PN-ISO 31000: 2012 *Zarządzanie ryzykiem – Zasady i wytyczne* oraz PN-ISO/IEC 27005: 2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*. W pierwszej z nich

podane są zasady i ogólne wytyczne dotyczące zarządzania ryzykiem. Norma ta może być stosowana przez wszystkie podmioty gospodarcze i administracyjne w ciągu całego okresu działalności. Poza tym może być stosowana niezależnie od typu ryzyka. Nie jest stosowana na potrzeby certyfikacji. Stanowi wskazówki do wdrożenia. W drugiej z wymienionych norm opisane są dobre praktyki i wskazówki dotyczące planowania i wdrażania zarządzania ryzykiem w ramach zarządzania bezpieczeństwem informacji. W normie podano stosowne wytyczne dla organizacji, a w szczególności wymagania dotyczące systemu zarządzania bezpieczeństwem informacji zgodnego z PN-ISO/IEC 27001.

Fazy procesu zarządzania ryzykiem w organizacji:

1. Faza planowania – ustanowienie kontekstu funkcjonowania systemu zarządzania ryzykiem w organizacji, tj. relacji zewnętrznych i wewnętrznych, środowiska prawnego, procesów biznesowych, organizacji, przepływów i sposobów przetwarzania informacji, zasobów ludzkich, lokalizacji i infrastruktury organizacji oraz innych aspektów. W tej fazie organizacja powinna mieć opracowaną, udokumentowaną oraz zatwierdzoną metodykę szacowania ryzyka, w której powinny być zawarte zasady postępowania z ryzykiem, zasady akceptacji ryzyka i wskazanie poziomu akceptowanego ryzyka.
2. Faza wykonania, która dotyczy wdrożenia planu postępowania z oszacowanym ryzykiem.
3. Faza sprawdzania (kontroli), która obejmuje proces ciągłego nadzoru (monitorowania) i sprawdzania ryzyka w organizacji. Proces ten można realizować poprzez audyty wewnętrzne oraz zewnętrzne, a także stosując system i procedury zarządzania incydentami.
4. Faza działania, która ma na celu utrzymanie sprawności i skuteczności systemu zarządzania bezpieczeństwem informacji i zarządzania ryzykiem w organizacji oraz doskonalenie tego systemu.

W normach nie przedstawiono żadnej określonej metodyki zarządzania ryzykiem w związku z ochroną informacji. Organizacja sama określa swoje podejście do zarządzania ryzykiem w zależności od zakresu SZBI, kontekstu zarządzania ryzykiem lub branży. W ramach struktur opisanych w normach można zastosować różne już istniejące metodyki.

Wymagania zawarte w normie PN-ISO/IEC 27005 powinny być brane pod uwagę przez kierownictwo organizacji, personel zajmujący się zarządzaniem ryzykiem w związku z zarządzaniem bezpieczeństwem informacji i strony zewnętrzne, które są zaangażowane w taką działalność. Norma ta stanowi rozwinięcie ogólnych koncepcji określonych w ISO/IEC 27001 i została opracowana w celu wsparcia wdrożenia zarządzania ryzykiem w zarządzaniu bezpieczeństwem.

Rys. 1. Fazy procesu zarządzania ryzykiem w organizacji

Norma ma zastosowanie do wszystkich typów organizacji (np. przedsiębiorstw, instytucji rządowych, organizacji non-profit).

Podstawowe terminy i definicje

Zrozumienie procesu zarządzania ryzykiem wymaga poznania i zrozumienia podstawowych terminów, które są używane do jego opisywania. Oto definicje tych terminów:

- ryzyko – prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów lub ryzyko – funkcja prawdopodobieństwa zdarzenia i jego konsekwencji;
- zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów lub skoordynowane kierowanie i zarządzanie organizacją z uwzględnieniem ryzyka;
- analiza ryzyka – systematyczne używanie informacji w celu zidentyfikowania źródeł i oszacowania ryzyka;
- ocena ryzyka – proces porównywania oszacowanego ryzyka z wyznaczonymi kryteriami w celu określenia wagi ryzyka;
- postępowanie z ryzykiem – proces wyboru i wdrażania środków modyfikujących ryzyko;
- ryzyko szczątkowe – ryzyko pozostające po procesie postępowania z ryzykiem;
- identyfikowanie ryzyka – proces znajdowania, zestawiania i charakteryzowania elementów ryzyka;
- szacowanie ryzyka – proces przypisywania wartości do prawdopodobieństwa i konsekwencji ryzyka;
- akceptowanie ryzyka – decyzja o zaakceptowaniu ryzyka.

Podatność a zagrożenie

Podatność jest często mylona z zagrożeniem. W rzeczywistości zagrożenie to potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub organizacji, a podatność to słabość zasobu lub grupy zasobów (aktywów), która może powodować zagrożenie.

W definicji podatności użyto terminu *zasób*, który oznacza wszystko, co ma wartość dla organizacji. Należy pamiętać, że podatność może spowodować zagrożenie. Sama nie powoduje szkód. Jest raczej właściwością powodującą, że w pewnych okolicznościach zasoby są zagrożone. W związku z podatnością zasobów, należy je nadzorować.

Różnicę pomiędzy zagrożeniem a podatnością na zagrożenie można wyjaśnić, posługując się przykładami. Brak ochrony fizycznej i technicznej obiektu może spowodować zagrożenie włamaniem lub napadem na obiekt. Brak odpowiedniego zarządzania i nadzoru nad konfiguracją sprzętu komputerowego może spowodować zagrożenie podmianą części składowych stacji roboczej i zagrożenie podsłuchem lub kradzieżą danych. Następstwem niewykonywania regularnie zapasowych kopii danych może być zagrożenie wystąpieniem braku ciągłości działania w przypadku awarii. Brak nadzoru nad niszczeniem dokumentów z informacjami wrażliwymi może spowodować zagrożenie uzyskaniem przez osoby nieuprawnione dostępu do tych informacji. Niewłaściwe procedury zatrudniania na stanowiskach, na których możliwy jest dostęp do informacji chronionych, powoduje zagrożenie ujawnieniem takich informacji.

Podsumowanie

Niniejsza część artykułu miała na celu podkreślenie znaczenia szacowania ryzyka oraz konieczności audytowania procesu zarządzania ryzykiem. Są to podstawy prawidłowego funkcjonowania systemu zarządzania bezpieczeństwem. Kolejna część będzie dotyczyć sposobów pomiaru ryzyka, wyboru sposobu postępowania z ryzykiem, wpływu analizy ryzyka na wybór sposobów zabezpieczenia procesów w organizacji oraz tego, co należy sprawdzić podczas audytu w związku z szacowaniem ryzyka.

Opracował
dr inż. Andrzej Wójcik
ekspert i rzeczoznawca ds. bezpieczeństwa technicznego i ochrony informacji
audytor ds. bezpieczeństwa biznesu
andrzejw@esinstal.pl

ZEUS

SERIA CZERWONA - DLA PROFESJONALISTÓW

WYSOKA JAKOŚĆ, BEZAWARYJNOŚĆ I ŁATWY MONTAŻ

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Zabezpieczanie posesji

Różne techniki detekcji

Maciej Prelich

Wybierając zabezpieczenia, np. system ochrony perymetrycznej, w celu ochrony własnej albo firmowej posesji użytkownicy mogą wybierać spośród wielu dostępnych rozwiązań, w których do wykrywania intruzów wykorzystuje się różne zjawiska fizyczne i techniki. Wiele z tych zjawisk i technik ma również inne zastosowania. Niektóre są powszechnie znane

Jednym z przykładów mogą być techniki mikrofalowe. Wykorzystuje się je w kolejnych generacjach barier oraz czujek dualnych, takich jak sprawdzony przez służby militarne Model 316 firmy SouthWest Microwave, ponieważ umożliwiają bardzo efektywną detekcję intruzów. Jednocześnie promieniowanie mikrofalowe jest obecne w wielu gospodarstwach domowych w znacznie prostszych formach – w bezprzewodowych sieciach Wi-Fi, Bluetooth oraz w kuchenkach mikrofalowych.

Innym przykładem są techniki wykorzystujące światło w zakresie podczerwieni. W systemach zabezpieczających stosowane są zarówno aktywne bariery wykorzystujące nadajniki i odbiorniki podczerwieni, jak i pasywne czujki podczerwieni wykrywające promieniowanie cieplne emitowane przez wszystkie ciała, których temperatura jest wyższa od temperatury otoczenia. W domach promieniowanie podczerwone jest wykorzystywane w pilotach sterujących telewizorami lub odtwarzaczami płyt.

Kolejnym przykładem jest zjawisko piezoelektryczne wykorzystywane w służących do zabezpieczania ścian, okien oraz ogrodzeń czujnikach piezodynamicznych, takich jak nowatorski system DEA Xensity, opisany dokładnie w numerze 4/2017 *Zabezpieczeń*. Najpopularniejszym i używanym na co dzień przedmiotem wykorzystującym to zjawisko jest zapalniczka piezoelektryczna – po naciśnięciu przycisku w zapalniczce powstaje iskra, która zapala paliwo. Uniwersalność oraz rozwój czujników, których działanie bazuje na zjawisku piezoelektrycznym, sprawiły, że mają one wiele różnych zastosowań (np. w urządzeniach medycznych, akcelerometrach w telefonach komórkowych, wtryskach paliwa w silnikach Diesla).

Skupmy się teraz na termowizji. Dzięki niej można wykryć obecność intruza przy braku choćby

najsłabszego oświetlenia światłem widzialnym. W tym celu stosuje się obrazowanie w paśmie głębokiej podczerwieni, które umożliwia rejestrację promieniowania cieplnego emitowanego przez ciała fizyczne w przedziale temperatur spotykanych w codziennych warunkach. Ze względu na sposób działania kamery termowizyjne szybko znalazły wiele zastosowań wojskowych oraz w systemach służących do ochrony obiektów o znaczeniu krytycznym (np. elektrowni, rafinerii, stacji przeładunkowych i fabryk). W naszej ofercie znajdują się produkty firmy FLIR będącej liderem w wytwarzaniu światowej klasy kamer termowizyjnych. Termowizja jest też wykorzystywana w medycynie (dzięki bezinwazyjności metody), w diagnozowaniu pracy maszyn, do oceny szczelności warstwy izolacyjnej budynków etc. Ponadto kamery termowizyjne są elementami zaawansowanych systemów uwierzytelniających użytkownika, umożliwiających np. odblokowanie telefonu dzięki trójwymiarowemu skanowi twarzy bądź sterowanie w grach interaktywnych za pomocą ruchów ciała.

Mam nadzieję, że powyższe przykłady dobrze uwidaczniają, jak wiele z zaawansowanych technik używanych do detekcji intruzów ma zastosowanie również w popularnych urządzeniach służących do innych celów – także tych, których używamy na co dzień. W praktyce zastosowanie tych technik zależy od różnych czynników, np. wymagań użytkownika (jeśli chodzi o skuteczność zabezpieczenia), budżetu przeznaczonego na system zabezpieczeń czy możliwości instalacji poszczególnych elementów. Nasi specjaliści zajmują się odpowiednią oraz fachową analizą umożliwiającą skonfigurowanie systemów dostosowanych do potrzeb nawet najbardziej wymagających klientów.

Maciej Prelich
Firma ATLine sp.j. Sławomir Pruski

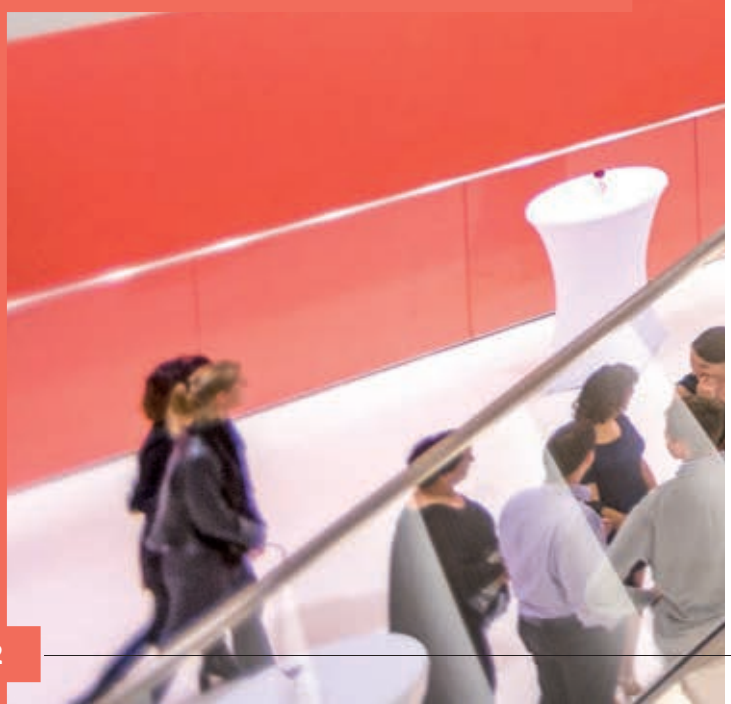
Systemy zabezpieczeń Bosch
w ICE Kraków Congress Centre

Bosch Security Systems

ICE Kraków Congress Centre to nowoczesne, światowej klasy centrum koncertowo-kongresowe. W obiekcie usytuowanym w jednym z najbardziej prestiżowych miejsc w Polsce – na wprost Zamku Wawelskiego – znajdują się trzy główne sale, mieszczące 1915, 600 i 300 osób, i wielofunkcyjna przestrzeń konferencyjna o powierzchni 550 m^2, którą można dowolnie dzielić za pomocą systemu mobilnych ścian, a także biura, garderoby artystów oraz powierzchnia komercyjna

Centrum kongresowe ICE Kraków Congress Centre zostało zaprojektowane z uwzględnieniem najwyższych standardów funkcjonalnych i akustycznych. Ze względu na różnorodność imprez i spotkań, jakie odbywają się na terenie obiektu (od koncertów do wielkich międzynarodowych konferencji) bezpieczeństwo ludzi i zasobów jest priorytetem. Firma Bosch dostarczyła systemy sygnalizacji pożarowej, systemy nagłośnieniowe, dźwiękowe systemy ostrzegawcze, systemy sygnalizacji włamania i napadu oraz systemy konferencyjne, które spełniają wysokie wymagania dotyczące bezpieczeństwa.

Rozwiązania firmy Bosch stanowią istotny element zabezpieczeń ICE Kraków Congress Centre. Za detekcję pożaru odpowiada modułowa centrala Bosch FPA w konfiguracji rozproszonej, wyposażona w punktowe i liniowe detektory dymu i temperatury. W reprezentacyjnych pomieszczeniach zostały zainstalowane płaskie czujki dekoracyjnie zlicowane z powierzchnią sufitu. W sumie firma Bosch dostarczyła do obiektu prawie 2000 czujek pożarowych.



Fot. Krakowskie Biuro Festiwalowe
(fot. W. Wandzel dla KBF, wandzelphoto.com)

W ICE Kraków Congress Centre zastosowano system nagłośnieniowy DSO Bosch Praesideo w konfiguracji rozproszonej. Perfekcyjną jakość dźwięku zapewniają głośniki Bosch, w tym zaawansowane głośniki hemisferyczne w atrium i w salach audytoryjnych.

Nadzór wizyjny w obiekcie bazuje na systemie zarządzania i rejestracji Bosch Video Management oraz kombinacji różnych kamer. Część z nich to nowoczesne 12-megapikselowe kamery panoramiczne z obiektywami typu rybie oko.

System sygnalizacji włamania i napadu w ICE Kraków Congress Centre bazuje na centrali Bosch MAP ze skutecznymi w działaniu detektorami sufitowymi i dualnymi.

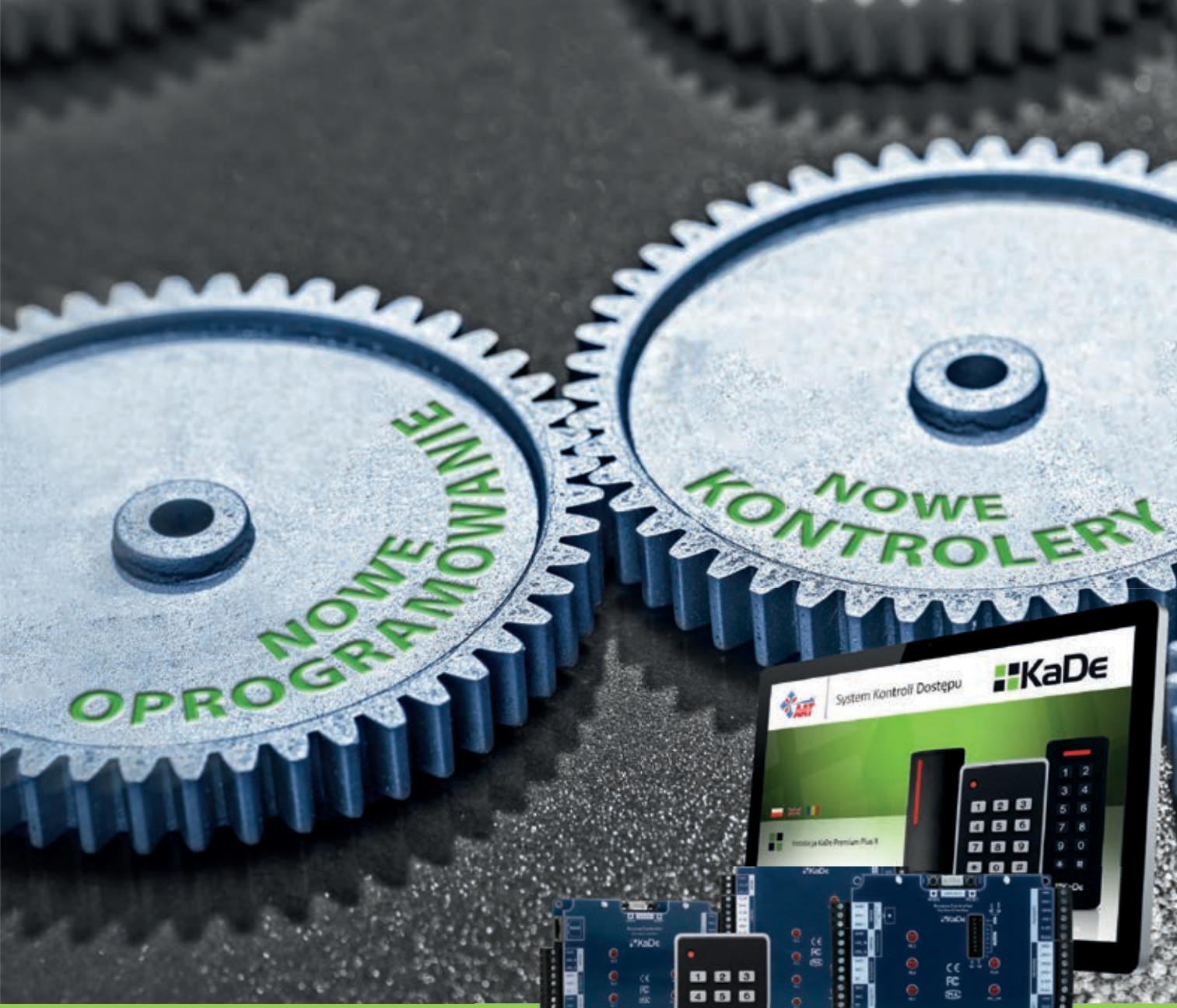
Fot. Krakowskie Biuro Festiwalowe
(fot. W. Wandzel dla KBF, wandzelphoto.com)

Dostępem do wskazanych pomieszczeń zarządza się za pomocą systemu KD firmy Bosch z kontrolerami IP serii AMC.

Bosch Building Integration System (BIS) umożliwia integrację i obsługę wszystkich systemów za pomocą jednej stacji operatorskiej, powiązanie zdarzeń i w efekcie skuteczne zarządzanie bezpieczeństwem w obiekcie.

W codziennym funkcjonowaniu ICE Kraków Congress Centre istotną rolę odgrywają zaawansowane systemy konferencyjne Bosch, takie jak system tłumaczeń symultanicznych Integrus czy system dyskusyjny DCN.

Bosch Security Systems



KaDe

NOWY SYSTEM KADE
IDEALNE DOPASOWANIE

MAPY OBIEKTU Z AKTYWNYMI, ANIMOWANYMI IKONAMI ELEMENTÓW SYSTEMU
GLOBALNY ANTI-PASSBACK

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

KaDe Premium Plus II

Program nadzorczy

KaDe

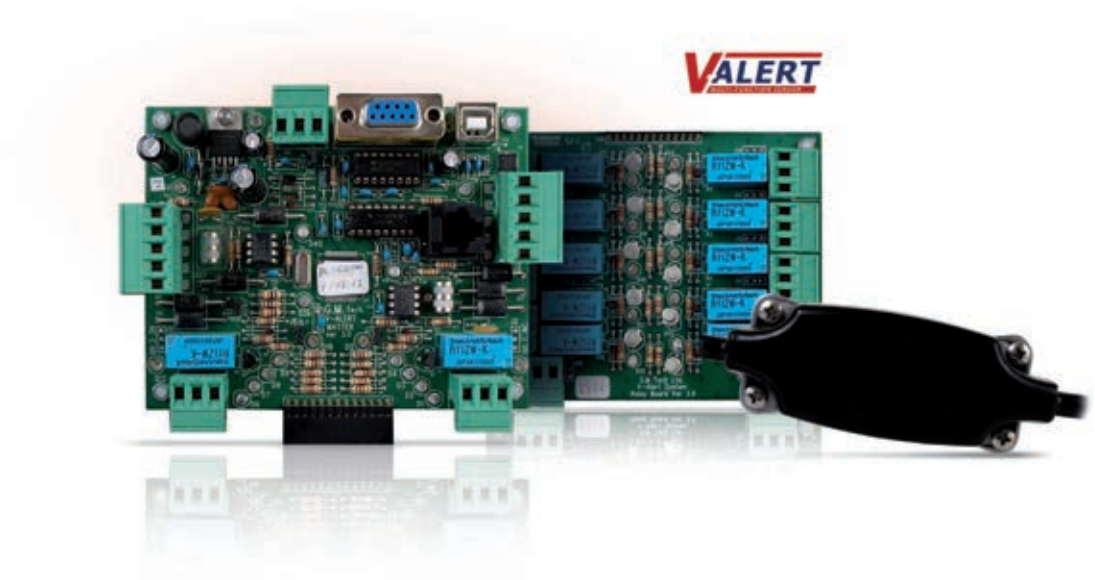
Program nadzorczy KaDe Premium Plus II jest przeznaczony do współpracy z kontrolerami standardowymi typu KDH-KS2012/24-IP/RS oraz kontrolerami zintegrowanymi KDH-KZ2000-IP-U i KDH-KZ2000-IP-M w trybie sieciowym. Program jest bardzo prosty w instalacji i posiada przyjazny interfejs graficzny dla operatora. Na uwagę zasługują zwłaszcza - wyświetlane na pulpicie operatora - okna „Dynamicznej pomocy", czyli podręcznej instrukcji. Program nadzorczy KaDe Premium Plus II przeznaczony jest do małych i średnich systemów.

Model	KaDe Premium Plus II
System operacyjny PC	Windows 7, 8, 10
Stacje operatorów systemu	1
Kontrolery	KDH-KS2012-IP, KDH-KS2024-IP, KDH-KS2012-RS, KS-1012-IP, KS-1024-IP, KS-1012-RS, KS-1024-RS, KDH-KZ2000-IP-U, KDH-KZ2000-IP-M, KZ-1000-IP-U, KZ-1000-IP-M
Liczba obsługiwanych kart	20000
Format obsługiwanych kart	26-40 bitów Wiegand
Typ obsługiwanych kart	dowolna technologia zgodna z czytnikiem
Poziomy dostępu	200
Harmonogramy	90
Tryby odryglowania drzwi	4
Tryb identyfikacji użytkownika	karta, kod dostępu, karta lub kod dostępu, karta i kod dostępu
Anti-Passback	lokalny/globalny
Raporty	filtrowane, zapis w formacie xls
Sekwencyjne odrygl. zarygl. drzwi	tak
Rejestracja czasu pracy	tak
Wizualizacja systemu na mapach obiektu	tak
Baza danych - import/export	tak
Monitoring „on-line"	tak
Wyświetlanie zdjęć użytkowników	tak
Dostęp po potwierdzeniu przez operatora	tak
Dostęp po użyciu wielu kart	tak

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. 22 546 05 46, faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

V-Alert
System ochrony obwodowej



System ochrony obwodowej V-Alert to wszechstronny system bezpieczeństwa oparty na elektronicznych czujnikach, zapewniający ochronę obwodową obiektów mieszkalnych, przemysłowych i wojskowych.

Model		Karta procesorowa V-Alert
Napięcie zasilania		9-14 V
Pobór prądu		50-250 mA
Liczba linii sensorowych		2
Liczba sensorów na linii sensorowej		maks. 50 sensorów (standard)
Komunikacja na linii sensorowej		RS-485
Komunikacja z PC		RS-232
Wymiary karty procesorowej (mm)		200 x 200
RTC (zegar czasu rzeczywistego)		godziny – minuty – sekundy
Tryb pracy		MASTER
Programowanie parametrów		oddzielnie dla osi X, Y (za pomocą V-AlertCOMM Settings Manager)
Sygnały wyjściowe	Za pomocą karty wyjść przekaźnikowych	- 4 wyjścia przekaźnikowe alarmowe dla każdej linii sensorowej - 1 wyjście przekaźnikowe dla przecięcia każdej linii sensorowej
	Komunikacja z PC	każdy sensor indywidualnie
Temperatura pracy		-30°C do 70°C
Wilgotność		20% do 95%

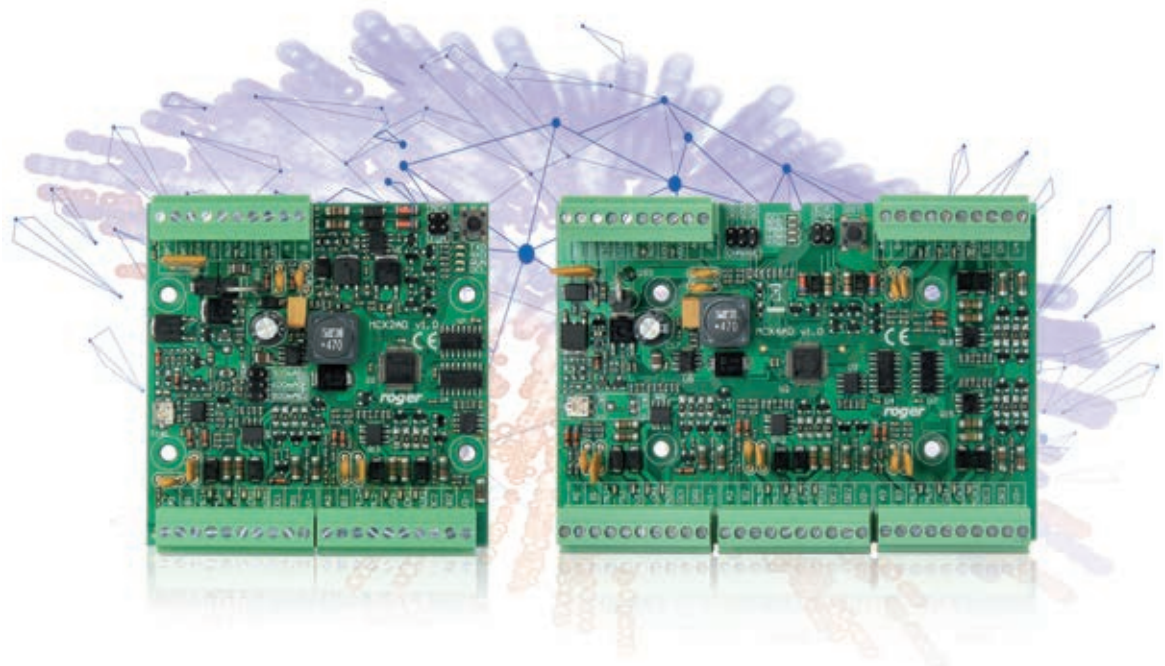
Model	Sensor V-Alert
Napięcie zasilania	8-13,8 V
Pobór prądu	10 mA
Komunikacja	RS-485
Liczba osi	2 (oś X, oś Y)
Metoda detekcji	Peak detect (wartość szczytowa)
Wymiary (mm)	20 x 50 x 105
Temperatura pracy	-30°C do 70°C
Wilgotność	10% do 95%
Tryb pracy	Slave

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. 22 546 05 46, faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

MCX2D/MCX4D

Ekspandery przejść do systemu RACS 5



MCX2D oraz MCX4D są ekspanderami we/wy przeznaczonymi do obsługi przejść w systemie RACS 5. Oprócz funkcji ekspandera, dany moduł pełni rolę dystrybutora zasilania i komunikacji oraz obsługuje rezerwowy akumulator. Dla każdego z obsługiwanych przejść ekspander oferuje 2 wejścia linii dozorowych, 2 wyjścia sterujące, interfejs komunikacyjny do czytników oraz dwa wyjścia zasilające. Obwody elektryczne przeznaczone do obsługi każdego z przejść są między sobą separowane elektrycznie, co powoduje, że wystąpienie awarii lub sabotażu na jednym z przejść nie ma wpływu na działanie pozostałych przejść. Ekspander jest zasilany z zewnętrznego zasilacza 13,8 V_{DC}, który jest jednocześnie źródłem zasilania zamków, czytników i innych elementów przejścia. Na każde z obsługiwanych przejść przewidziano prąd zasilania na poziomie 1,2 A. Ekspander współpracuje z akumulatorem rezerwowym, który w zależności od potrzeb może być ładowany regulowanym prądem w zakresie 0,3-0,9 A. Połączenia elektryczne z modułem są realizowane za pośrednictwem wyjmowanych zacisków śrubowych, które ułatwiają wykonanie połączeń elektrycznych w czasie instalacji jak i w przypadku konieczności wymiany modułu.

Charakterystyka	MCX2D	MCX4D
Dystrybucja zasilania do 4 przejść	+	+
Dystrybucja magistrali komunikacyjnej	+	+
Wejścia EOL/2EOL	4	8
Wyjścia 12 V/1 A	4	8
Wyjścia zasilania 12 V/1 A	2	4
Wyjścia zasilania 12 V/0,2 A	2	4
Interfejs komunikacyjny RS485 do kontrolera dostępu	+	+
Zabezpieczenie przed głębokim rozładowaniem akumulatora	+	+
Raportowanie stanów zasilania do kontrolera dostępu	+	+
Ładowanie akumulatora prądem 0,3 A, 0,6 A lub 0,9 A	+	+
Zasilanie z zewnętrznego zasilacza	13,8 V_{DC}/3 A	13,8 V_{DC}/5 A

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

MCT82M-IO-HR

Hotelowy czytnik zbliżeniowy do systemu RACS 5

MCT82M-IO-HR jest odmianą czytnika MCT82M-IO-BK przeznaczoną do kontroli dostępu do pokoi hotelowych funkcjonujących w ramach systemu kontroli dostępu i automatyki budynkowej RACS 5. Terminal umożliwia identyfikacje użytkowników za pośrednictwem kart zbliżeniowych standardu ISO 14443A/B i MIFARE. Identyfikacja może odbywać się zarówno za pośrednictwem fabrycznego numeru seryjnego numeru karty (CSN), jak i numeru karty zaprogramowanego w szyfrowanych sektorach karty (SSN). Na panelu frontowym czytnika dostępne są 4 wskaźniki sygnalizacyjne LED oraz przycisk dzwonka. Wskaźniki LED przeznaczone są do typowych sygnalizacji hotelowych: nie przeszkadzać, zamówienia serwisu sprzątającego oraz gastronomicznego, a także przywołania asysty pracownika hotelu. Terminal jest wyposażony w zestaw 3 linii wejściowych oraz 3 linii wyjściowych, w tym jednego wyjścia przekaźnikowego. Zarówno linie wejściowe jak i wyjściowe mogą być skonfigurowane do dowolnych funkcji, w tym obsługi czujnika otwarcia drzwi oraz sterowania zamkiem. Po doposażeniu pokoju hotelowego w instalowany wewnątrz pokoju czytnik z kieszenią MCT82M-IO-CH, można w ramach systemu RACS 5 uzyskać podstawowy zestaw urządzeń realizujących typowe wymagania w zakresie kontroli dostępu i automatyki w pokojach hotelowych. Terminal MCT82M-IO-HR jest zgodny z linią wzorniczą QUADRUS.

Charakterystyka

- Terminal MIFARE Ultralight/Classic/Plus/DESFire
- 4 wskaźniki LED
- Buzzer z regulowanym poziomem głośności
- Sensoryczny klawisz dzwonka
- 3 linie wejściowe
- 2 wyjście tranzystorowe
- 1 wyjście przekaźnikowe NO/NC
- Interfejs komunikacyjny RS485
- Zasilanie 12 V_{DC}
- Wymiary 130 x 45 x 22 mm
- Znak CE

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46; faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

D PROD S

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. Antoniuk Fabryczny 22, 15-741 Białystok
tel. 85 688 32 33
tel./faks 85 688 32 34
e-mail: aat.bialystok@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, 361 16 33
e-mail: aat.kielce@aat.pl

ul. Biskupińska 14, 30-732 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, 662 06 61
e-mail: aat.poznan@aat.pl

Al. Niepodległości 606/610, 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

D PROD PROJ

ALARMNET BORKIEWICZ 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

D PROD PROJ S

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

D PROD PROJ S

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

I PROD PROJ

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
www.assaabloy.com.pl

D I PROJ S

FIRMA ATLINE SPÓŁKA JAWNA SŁAWOMIR PRUSKI
ul. Franciszkańska 125
91-845 Łódź
tel. 42 236 30 19; faks 42 655 20 99
e-mail: biuro@atline.pl
www.atline.pl

D I PROD PROJ

BOSCH SECURITY SYSTEMS
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 40 00
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl

D S

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

D I PROJ

bt electronics Sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. 12 429 36 16; faks 12 410 85 11
e-mail: bte@bte.pl
www.bte.pl

I PROD PROJ S

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90; faks 22 633 90 60
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

D PROD PROJ S

CMA MONITORING
a Viasat Group Company

CMA Monitoring Group Sp. z o.o.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888; faks 22 546 0 619
e-mail: info@cma.com.pl
www.cma.com.pl

Oddziały:
ul. Składowa 2, 41-902 Bytom
tel. 32 388 09 50; faks 32 388 09 60

ul. Zatorska 36, 51-215 Wrocław
tel. kom. 697 972 558
faks 71 341 16 26

Biura handlowe:
ul. Nowy rynek 2, 62-002 Suchy Las k/Poznania
tel. kom. 601 203 664, 601 410 979
faks 61 861 40 51

ul. Hallera 140, lok. 124, 80-416 Gdańsk
tel kom. 693 694 339

CONTROL SYSTEM FMN

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17/18; faks 22 855 00 19
e-mail: cs@cs.pl
www.cs.pl

a)hua TECHNOLOGY

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2, Lisbon Building, Lobby II
02-823 Warszawa
tel. 22 395 74 00; faks 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

DG ELPRO

DG ELPRO Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85; faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.pl

DYSKRET

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

EBS
CREATING A SENSE OF SECURITY
SINCE 1989

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 518 84 00; faks 22 518 84 99
e-mail: sales@ebs.pl
www.ebs.pl

ELPROMA SECURITY

PHU ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel. kom. 606 270 756
tel. 22 398 96 53
e-mail: elproma@elproma.pl
www.elproma.pl

ELSTECH

ELSTECH
os. Złota Podkowa 6/4
31-352 Kraków
tel. kom. 570 400 537, 570 400 538;
faks 12 350 45 03
e-mail: info@elstech.pl
www.elstech.pl

eltrox.pl

Eltrox.pl
ul. Główna 23
42-280 Częstochowa
tel. 34 341 14 61
tel. kom. 517 015 471
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Hynka 6/2, 80-465 Gdańsk
tel. kom. 517 015 441
e-mail: gdansk@eltrox.pl

ul. 6 sierpnia 14, 90-416 Łódź
tel. 42 632 31 24
e-mail: lodz@eltrox.pl

ul. Brynowska 65/4, 40-584 Katowice
tel. 32 203 50 73
e-mail: katowice@eltrox.pl

ul. Wybickiego 42A, 31-302 Kraków
tel. kom. 501 945 239
e-mail: krakow@eltrox.pl

ul. Dmowskiego 2/1, 45-365 Opole
tel. kom. 501 945 246
e-mail: opole@eltrox.pl

ul. Stablewskiego 31/3, 60-223 Poznań
tel. kom. 504 904 710
e-mail: poznan@eltrox.pl

ul. Wyszyńskiego 26, 70-203 Szczecin
tel. 91 434 78 72
e-mail: szczecin@eltrox.pl

ul. Remiszewska 1/7B, 03-550 Warszawa
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

ul. Łopuszańska 22, 02-220 Warszawa
tel. kom. 506 601 006
e-mail: warszawa2@eltrox.pl

ul. Komandorska 53R, 50-258 Wrocław
tel. kom. 503 127 533
e-mail: wroclaw@eltrox.pl

EST EUROPEAN SECURITY TRADING
POLSKA

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
ul. Wilcza 54a lok. 1
00-679 Warszawa
tel. 22 629 53 49
e-mail: kontakt@estpolska.pl
http://europeansecuritytrading.com/pl

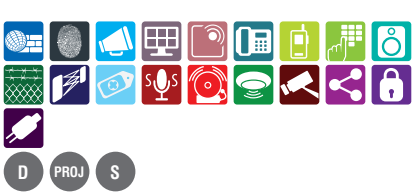
EWIMAR Sp. z o.o.
ul. Konarskiego 84
01-355 Warszawa
tel. 22 691 90 65
e-mail: handel@ewimar.pl
www.ewimar.pl

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

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

HANWHA TECHWIN EUROPE LTD.
Biuro w Polsce
ul. Posag 7 Panien 1
02-495 Warszawa
e-mail: hte.poland@hanwha.com
www.hanwha-security.eu

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



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

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

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

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
02-672 Warszawa
tel. 22 549 23 30
e-mail: info@legrand.com.pl
www.legrand.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
e-mail: info@micronix.pl
www.micronix.pl

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

PROFICCTV Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.profisystems.pl

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

D I PROD PROJ S

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

D

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16; faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07; faks 12 379 34 10
www.ropam.com.pl

D PROD S

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44A
02-672 Warszawa
tel. 22 33 00 620; faks 22 33 00 624
e-mail: jolanta.paska@schrack-seconet.pl
www.schrack-seconet.pl

PROD PROJ S

Oddziały:
ul. M. Gomółki 2, 80-279 Gdańsk
tel. 58 526 35 70
e-mail: gdansk@schrack-seconet.pl

ul. Jasnogórska 23 lok. 17
(wejście od ul. Stawowej)
31-358 Kraków
tel. 12 637 11 74
e-mail: krakow@schrack-seconet.pl

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

ul. Mydlana 1, 51-502 Wrocław
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

TAP- Systemy Alarmowe Sp. z o.o.
ul. Tatrzańska 8
60-413 Poznań
tel./faks 61 677 48 00
e-mail: tap@tap.com.pl
www.tap.com.pl

D PROJ S

Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00
e-mail: techom@techom.com
www.techom.com

B C S

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

B D PROD PROJ

WINKHAUS POLSKA BETEILIGUNGS
Spółka z ograniczoną odpowiedzialnością Sp.K.
ul. Przemysłowa 1
64-130 Rydzyna
tel. 65 525 57 00
faks 65 525 58 00
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

D PROD

Legenda

Kategorie*

- bezpieczeństwo IT
- biometria
- DSO
- monitoring
- ochrona fizyczna
- RFID
- systemy domofonowe i wideodomofonowe
- systemy komunikacyjne
- systemy kontroli dostępu
- systemy nagłośnieniowe
- systemy ochrony peryferyjnej
- systemy ochrony zewnętrznej
- systemy przeciwkradzieżowe
- systemy przywoławcze
- systemy sygnalizacji pożarowej
- systemy sygnalizacji włamania i napadu
- systemy telewizji dozorowej
- systemy zintegrowane
- zabezpieczenia mechaniczne
- zasilanie

Działalność*

- B badania
- C certyfikacja
- D dystrybucja
- I instalacja
- PROJ projektowanie
- PROD produkcja
- S szkolenia

* Szybkie wyszukiwanie przez filtrowanie na naszej stronie www.zabezpieczenia.com.pl

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Arkadiusz Milka
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Andrzej Wójcik

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, skład i łamanie
Piotr Przybylski

Adres redakcji
ul. Przy Bażantarni 13
02-793 Warszawa
tel. 22 670 09 19
faks 22 649 97 19
www.zabezpieczenia.com.pl

Wydawca
AAT HOLDING S.A.
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

Dostępne formy reklamy

Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

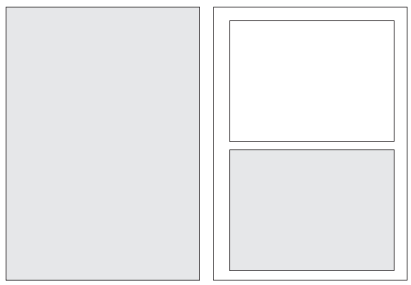
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

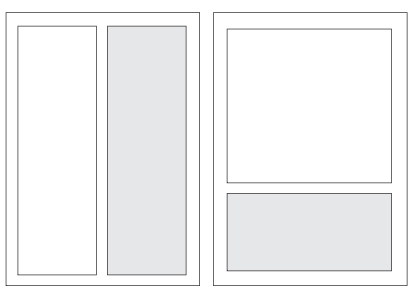
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

Udostępniamy również powierzchnię reklamową na naszej stronie internetowej http://www.zabezpieczenia.com.pl



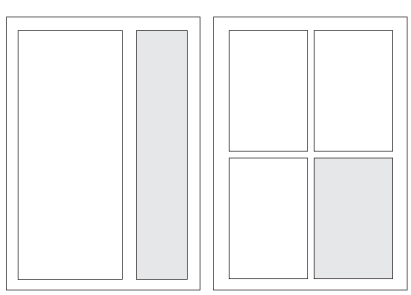
cała strona
(200 x 282 mm + 3mm spad)

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

BOSCH
Technologia bliżej nas

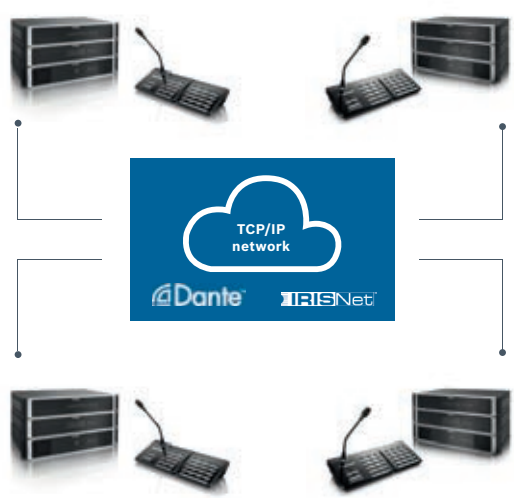
Centrala Dźwiękowego Systemu Ostrzegawczego

PAVIRO w wersji sieciowanej

Korzystając z technologii IP system PAVIRO zapewnia teraz oprócz jeszcze większej elastyczności, niezawodne i bezpieczne rozwiązanie łączenia systemów w sieć, zachowując przy tym wysoką jakość dźwięku – niezależnie od odległości i wielkości obiektu.

PAVIRO wyposażone w opcjonalny interfejs sieci OMNEO OM-1 (szyfrowana transmisja danych i sygnałów audio bazująca na DANTE) umożliwia transmisję do 16 kanałów audio pomiędzy kontrolerami PVA-4CR12. Cztery kontrolery połączone w jedną sieć tworzą jeden system do 984 stref, z mocą do 164 000W.

Sieciowa konfiguracja pozwala na stworzenie nadmiarowego połączenia (ring) oraz nadmiarowej sieci TCP/IP (dwie niezależne sprzętowo sieci z topologią typu ring dla każdej).



Router 24-strefowy
z czterema kanałami

Dwukanałowy wzmacniacz
2x500 W, klasa D

Sterownik z cyfrowym procesorem dźwięku (DSP) dla pojedynczego systemu i sieciowanego PAVIRO

Stacja wywoławcza

Rozszerzenie stacji wywoławczej


securex®
POLAND
Międzynarodowe Targi Zabezpieczeń
23-26.04.2018
POZNAŃ
Zabezpiecz
swój sukces!
www.securex.pl