CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(64)/2008

ZABEZPIECZENIA

10 lat za nami

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

W NUMERZE:

Panasonic
ideas for life

Przetwornik CCD 1,3 Megapiksela, Pozwoli Ci Zobaczyć Więcej

Kamera megapikselowa

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

* Porównanie obrazów z kamer konwencjonalnej i megapikselowej i-Pro

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

Megapikselowa kamera sieciowa typu dzień/noc
WV-NP304

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

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

IP

Progresywne wyjście wideo

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

ABS (Adaptive Black Stretch)

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

Focus Assist

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

Terabajtowa pojemność dyskowa oraz precyzyjny monitoring

Sieciowy rejestrator dyskowy
WJ-ND400

Multikanałowy wideodekoder High Definition
WJ-GXD400

i-Pro Network Surveillance System

i-pro

http://panasonic.net/security/

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

Spis treści

A to wszystko na jednej karcie... 32

Blaski i cienie monitoringu IP – przykład negatywny 36

Monitory nowej generacji dla centrów nadzoru – seria LCD 400 marki NOVUS 58

Harmony. Zintegrowany system zarządzania personelem 76

Gunnebo zdobywa zamówienie
z międzynarodowego portu lotniczego w Bahrainie

Grupa Gunnebo otrzymała zamówienie na dostawę **bramek imigracyjnych ImmSec** do wzmocnienia poziomu bezpieczeństwa w międzynarodowym porcie lotniczym w Bahrainie. Zamówienie to uzyskano, gdyż istniejące zarówno w Wielkiej Brytanii, jak i w Japonii instalacje systemów imigracyjnych sprawdziły się tam w sposób rozstrzygający.

ImmSec jest pewnym i efektywnym systemem kontrolnym, który w danym momencie pozwala na przejście przez bramkę tylko jednej osobie. Zamówienie wstępne dotyczy czterech przejść próbnych ze zintegrowanymi chipowymi kartami identyfikacyjnymi, biometrycznym czytnikiem odcisków palców i dwoma monitorami LCD oraz z unikatowym systemem TDAR, służącym do wykrywania pojedynczych osób i pozostawionego bagażu. Zamówienie otrzymano we współpracy z firmą Securicore, lokalnym partnerem Gunnebo w Bahrainie.

– Wierzymy, że ImmSec ma znaczny potencjał na przejściach, na których wymaga się zarówno szybkiego przepływu ludzi jak i zapewnienia wysokiego poziomu bezpieczeństwa, takich jak punkty kontroli imigracyjnej – mówi Göran Gezelius, prezes i szef Gunnebo AB. – *Wszystkie rozwiązania identyfikacji biometrycznej wymagają uprzedniego zaprogramowania dokumentów identyfikujących, ale za to pozwalają na ekstremalnie szybkie przejście osób posiadających biometryczne dokumenty podróży przez punkty kontrolne.*

Instalacja pierwszych czterech bramek rozpoczęła się we wrześniu 2008 roku, a zamówienie może być rozszerzone na tego typu urządzenia do całego portu lotniczego.

Rząd Bahrainu wprowadził identyfikacyjne karty chipowe, aby ułatwić codzienną pracę i zintegrować wszystkie służby obsługi obywateli na jednej platformie. W związku z tym projektem rząd zdecydował się na wyposażenie portu lotniczego w Bahrainie w elektroniczne bramki imigracyjne. Oznacza to, że **Bahrain może być pierwszym krajem** zezwalającym swym obywatelom na opuszczenie kraju i powrót przy zastosowaniu **automatycznych biometrycznych procedur imigracyjnych.**

ImmSec to unikatowy system Gunnebo do automatyzacji tych procedur w portach lotniczych i morskich oraz na lądowych przejściach granicznych. System detekcyjny identyfikuje pojedyncze i zbiorowe konfiguracje ludzi, a także bagaż, niemowlęta i dzieci. Zintegrowany system detekcji weryfikuje obecność pojedynczej osoby oraz osób oszukańczo próbujących naruszać imigracyjne procedury bezpieczeństwa.

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

Sensormatic przejmuje Vue Technology

Sensormatic Electronics Corporation, firma należąca do **Tyco International**, ogłosiła przejęcie **Vue Technology** (Vue), wiodącego dostawcy oprogramowania wykorzystywanego do prowadzenia inwentaryzacji towarów przy wykorzystaniu technologii RFID. Przejęcie Vue wpisuje się w strategię firmy Sensormatic, która chce oferować swoim klientom zintegrowane rozwiązania w sektorze handlu detalicznego. Technologia firmy Vue obejmuje oprogramowanie, punkty odczytu RFID oraz radiowe urządzenia sieciowe, umożliwiające dokonywanie inwentaryzacji w czasie rzeczywistym. Włączenie takiej infrastruktury RFID do portfolio sprzętowych rozwiązań firmy Sensormatic w dziedzinie systemów przeciwkradzieżowych oraz innych technologii czujnikowych umożliwi sklepom i sieciom handlowym zastosowanie RFID w swoich obiektach, co polepszy w nich poziom kontroli i zabezpieczenia oraz stopień wglądu w stany magazynowe, przyczyniając się do zwiększenia efektywności operacyjnej przedsiębiorców.

Korzystając z platform RFID firmy Sensormatic, oprogramowania i sieciowych rozwiązań Vue, możliwości serwisowych i w zakresie sprzedaży globalnej **ADT** oraz sieci integratorów Vue, przedsiębiorcy prowadzący handel detaliczny będą mogli skorzystać na wzroście integralności danych na poziomie przedmiotowym i dokładniej prześledzić drogę towaru z magazynu do punktów kasowych, wykorzystując innowacyjną technologię wieloczujnikową.

– Vue zyskuje dostęp do zasobów firmy Sensormatic w zakresie rozwoju produktów oraz do globalnych możliwości dostawczych Tyco – powiedział **Robert Locke**, szef Vue Technology.

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

Counter Terror Expo kieruje dyskusję na zagrożenia terrorystyczne

– Mimo faktu, że poza polami bitwy w Iranie i Afganistanie nie było większych ataków terrorystycznych przeciwko celom Zachodu przez ponad rok, błędem byłoby zakładać, że zagrożenie takimi atakami zniknęło – twierdzi **Niche Events**, organizator Counter Terror Expo. Jest to jasne przesłanie, uwidocznione przez rekordowe zainteresowanie wystawców i delegatów na nadchodząca **imprezę Counter Terror Expo 2009 (CTX09), która odbędzie się w prestiżowym centrum QE11 w Londynie w dniach 10 i 11 lutego następnego roku.**

Ponad 75 światowych ekspertów w dziedzinie antyterroryzmu zbierze się podczas CTX09, aby dyskutować nad obecną naturą zagrożenia, badać trendy, identyfikować potencjalne trajektorie zagrożeń i pomagać w znajdowaniu możliwych rozwiązań przeciwdziałających wszelkim przejawom ofensywy grup terrorystów chcących spowodować maksimum szkód i zniszczeń.

– Takie wydarzenia, jak 11 września, Bali, Madryt, zamachy bombowe w metrze i autobusach londyńskich czy ataki na port lotniczy w Glasgow przypominają, że zagrożenie terroryzmem nigdy nie jest dalekie – komentuje **Peter Jones**, dyrektor imprezy CTX09. – *Wydarzenia ostatnich lat nauczyły nas wiele jeśli chodzi o to, jak działają grupy terrorystyczne, ale także zaskoczyły łatwością, z jaką zmieniają one w mgnieniu oka swoją taktykę i kierunki działania. Te wydarzenia sprowadziły nas także do kwestii przeciwdziałania aktom terroryzmu* – powiedział Peter Jones. – *W następstwie zarówno ataków z 11 września w Stanach Zjednoczonych, jak i ataków z 7 lipca w Wielkiej Brytanii odkryto, że różne części społeczności służb zapewniających bezpieczeństwo posiadły pewną wiedzę na temat niektórych terrorystów, ale z tego czy innego powodu zaniedbały przekazania tej informacji swoim odpowiednikom działającym gdzie indziej. Dzielenie się wiedzą jest żywotnym wymogiem w zapobieganiu terroryzmowi* – dodaje Jones.

CTX09 obejmuje zarówno **dwudniowy program konferencji** na wysokim poziomie, na którą przybędą eksperci oraz inni praktycy i dostawcy rozwiązań w zakresie antyterroryzmu w celu ułatwienia otwartej wymiany poglądów i wypracowania pomysłów na przeciwdziałanie zagrożeniom ze strony międzynarodowego terroryzmu, jak i **warsztaty specjalistyczne**, zapewniające forum, na którym delegaci będą mogli badać najnowsze dostępne rozwiązania technologiczne do zwalczania zagrożeń ze strony globalnego terroryzmu. CTX09 to także unikatowa **wystawa**, przedstawiająca najświeższe specjalistyczne produkty w zakresie zabezpieczeń i przełomowe rozwiązania w metodach przeciwdziałania zagrożeniu terrorystycznemu.

Zróżnicowany **program konferencji** obejmuje m.in. następujące tematy:

- kontrola granic oraz imigracja,
- współpraca międzyagencyjna i dzielenie się informacją,
- polityka antyterrorystyczna,
- współpraca międzynarodowa,
- transport,
- infrastruktura i usługi komunalne.

Warsztaty specjalistyczne skupią się na problematyce:

- dzielenia się informacją i wiedzą,
- przemytu ludzi i handlu narkotykami,
- technik niewidocznej inwigilacji,
- wykrywania ukrytej broni,
- wykrywania ciekłych materiałów wybuchowych,
- broni chemicznej i biologicznej,
- zagrożeń wewnętrznych,
- bezpieczeństwa lotniczego.

– Londyn widział w ostatnich czasach więcej terrorystycznych potworności niż mogłoby przypadać mu w udziale i jest to właściwe, że CTX09 będzie się odbywać właśnie tam, w pobliżu brytyjskich korytarzy władzy przy Whitehall (Whitehall to ulica w Londynie, w pobliżu której położone są brytyjskie budynki rządowe – przyp. redakcji). *Poza tym Londyn będzie gościł w 2012 roku największą sportową imprezę, igrzyska olimpijskie.* ***Ważnym tematem CTX09 będzie bezpieczeństwo imprez*** *na tak wielką skalę i mamy nadzieję, że dyskusja na ten temat przyczyni się do zapewnienia tego, że Igrzyska Olimpijskie 2012 będą najbezpieczniejszą olimpiadą w historii* – podsumowuje Peter Jones.

Z racji tego, że powierzchnia jest obecnie na wagę złota, firmy pragnące wystawiać się na CTX09 powinny jak najszybciej skontaktować się z organizatorami, aby uniknąć rozczarowania. Przewiduje się, że liczba delegatów będzie szybko piąć się w górę, więc tym osobom, które wykazują profesjonalne zainteresowanie uczestnictwem w imprezie, przypomina się o potrzebie zarezerwowania miejsca tak wcześnie, jak tylko jest to możliwe.

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

System nagłośnienia SX-2000 na stadionie Lechii Gdańsk

Z przyjemnością informujemy, iż firma **Ambient System** we wrześniu bieżącego roku zaprojektowała oraz dostarczyła na stadion **Lechii Gdańsk** (zespół grający w ekstralidze) kompletny system nagłośnienia, mający funkcje niezbędne do przeprowadzenia ewakuacji z obiektu.

Warto podkreślić, iż zastosowano najnowszy system na rynku audio – **SX-2000**, ten sam, który pracuje na stadionie olimpijskim **Ptasie Gniazdo w Pekinie.**

Z systemem SX-2000 współpracują szerokopasmowe zestawy głośnikowe dalekiego zasięgu, zapewniające wysoką jakość przetwarzania programu muzycznego i bardzo dobrą zrozumiałość mowy.

Bezpośr. inf. Ambient System

Nominacje do nagród czasopisma Detektor International w zakresie systemów zabezpieczeń

Podczas bankietu zorganizowanego dla ponad 900 profesjonalistów z branży zabezpieczeń na ostatniej **wystawie Skydd w Sztokholmie** ogłoszono nominacje do nagród czasopisma ***Detektor International***. Redaktor naczelny czasopisma **Lennart Alexandrie** nazwał tę imprezę „największym obiadem z okazji rozdania nagród na świecie".

Finał odbędzie się podczas bankietu organizowanego przy okazji wystawy **SECTECH w Kopenhadze (19–20 listopada br.)**, kiedy to zostaną wyłonieni zwycięzcy poszczególnych kategorii. Zostaną oni nagrodzeni indywidualnymi szklanymi rzeźbami znanego w świecie rzeźbiarza tworzącego w szkle **– Bertila Valliena.**

Poniżej lista nominowanych produktów.

Kategoria kontroli dostępu:

- **iLoq**, elektroniczny system zamykający fińskiej firmy iLoq,
- **RKL55**, czytnik kart chipowych firmy HID,
- **RF30EM**, bezprzewodowy czytnik systemu Bewator Entro V.6.0 z Siemens Building Technology - Security Products Division,
- **Diadem**, czytnik biometryczny łączący rozpoznawanie twarzy i mowy słoweńskiej firmy TAB Systems.

Kategoria systemów alarmowych i detektorów:

- **Hemi-Directional Loudspeaker**, głośnik przeznaczony do alarmu głosowego z Bosch Security Systems,
- **Galaxy Dimension**, centrala alarmowa z pełną kontrolą dostępu firmy Honeywell,
- **T5000**, kamera detekcyjna firmy ThruVision.

Kategoria telewizji dozorowej:

- **Axis P3301**, kamera sieciowa firmy Axis Communications,
- **IVA 3.5**, rozwiązanie inteligentnego systemu wizyjnego z Bosch Security Systems,
- **NSR-1000 series**, sieciowy serwer do systemów dozoru wizyjnego firmy Sony,
- **Q22**, kamera sieciowa z kątem podglądu 360 stopni firmy Mobotix.

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

Bosch wprowadza nowe nadajniki VideoJet X SN z obsługą inteligentnej analizy obrazu (IVA)

Urządzenia dostępne są w wersji 1-, 2- lub 4-kanałowej

W odpowiedzi na rosnące zapotrzebowanie rynku na „inteligencję w urządzeniu końcowym" **Bosch Security Systems** wprowadza **nową serię sieciowych nadajników wizyjnych** o wysokich parametrach – **VideoJet X SN**. W celu oszczędzania zasobów systemowych analiza obrazu przenoszona jest do urządzenia końcowego w sieci.

W nadajniki wbudowane jest oprogramowanie do wizyjnej analizy obrazu Bosch IVA 3.5. Dzięki temu nadajniki są w stanie samodzielnie wykrywać podejrzane zachowanie, np. długotrwałe przebywanie w określonym obszarze, pozostawienie obiektu w scenie, usunięcie obiektu oraz przekroczenie linii. Wspomniane funkcje, dostępne jako opcja wymagająca licencji, bazują na wcześniejszych wersjach oprogramowania. Możliwości wykrywania w nadajnikach VideoJet X SN zostały jednak znacznie poszerzone, m.in. o nowe możliwości filtrowania zdarzeń w oparciu o kolor obiektu. Kolor obiektu, a nawet kombinacja kolorów, może stanowić kryterium wykrywania. Zestaw filtrów został rozszerzony także o nowe wszechstronne funkcje w rodzaju alarmu przekroczenia linii oraz filtrowania trajektorii obiektu. W celu wyeliminowania fałszywych alarmów, wywoływanych np. przez małe zwierzęta, można użyć także filtru wielkości i prędkości.

W połączeniu z kamerami analogowymi i cyfrowymi rejestratorami wizyjnymi nowe nadajniki zapewniają najnowocześniejszą „analizę obrazu na miejscu" – prosty sposób na wprowadzenie inteligencji do istniejących systemów CCTV opartych na kamerach analogowych.

Nadajniki dostępne są w wersji 1-, 2- lub 4-kanałowej. Urządzenia przesyłają przez sieć sygnał wizyjny w formacie MPEG-4 z maksymalną pełną prędkością 25 obrazów (PAL) lub 30 obrazów (NTSC) na sekundę w rozdzielczości 4CIF na każdy kanał wizyjny.

VideoJet X SN oferuje również kilka opcji zapisu, począwszy od lokalnego zapisu na kartach pamięci Compact Flash czy zewnętrznych dyskach twardych dołączonych przez port USB po zapis w sieciowych macierzach RAID za pośrednictwem interfejsu iSCSI (*Internet Small Computer System Interface*) lub w scentralizowanym sieciowym rejestratorze wizyjnym NVR (*Network Video Recorder*). Opcja zapisu iSCSI RAID oferuje zasadnicze korzyści: pełną elastyczność w rozmieszczeniu urządzeń iSCSI w sieci oraz łatwą skalowalność systemu. Oznacza to prostszy i znacznie bardziej niezawodny łańcuch zapisu w porównaniu ze standardowymi rozwiązaniami opartymi o sieciowe rejestratory wizyjne.

Nadajniki serii VideoJet X SN są kompatybilne z oprogramowaniem *Bosch Video Recording Manager* (VRM). Oprogramowanie to zapewnia pełną kontrolę nad dyskami macierzy iSCSI RAID, w tym, w przypadku awarii napędu, automatyczne przekierowanie zapisywanego sygnału wizyjnego do alternatywnych urządzeń iSCSI. Dodatkowo oprogramowanie VRM umożliwia inteligentne wyszukiwanie metadanych na potrzeby dowodowe, tj. ciągów tekstowych składających się ze słów kluczowych opisujących określone scenariusze. Przesyłane są one razem z obrazem na nośnik zapisu. Wyszukiwanie na potrzeby dowodowe z użyciem metadanych jest znacznie szybsze niż żmudne, wielogodzinne przeglądanie zapisanego materiału. Stanowi to jedną z kluczowych zalet przesunięcia inteligencji do urządzenia końcowego.

Najnowocześniejsze nadajniki VideoJet X SN zastępują nadajniki serii VideoJet 10. Nowe modele mają profil przybliżony do starszej serii, dzięki czemu pasują do tego samego systemu umieszczonego w szafie typu *rack*. Umożliwiają jednocześnie zwiększenie funkcjonalności systemu monitoringu oraz jego dalszą rozbudowę.

Bezpośr. inf. Emilia Dobies
Bosch Security Systems

Coraz bezpieczniej na polskich drogach

Firmy **Bosch Security Systems** oraz Neurosoft (dostawca oprogramowania) zostały wybrane do wdrożenia pilotażowego projektu **CONNECT.**

CONNECT jest programem finansowanym przez Unię Europejską. Poprzez rozwój i wdrożenie innowacyjnych działań z zakresu ITS (ang. *Intelligent Transport Systems* – Inteligentne Systemy Transportowe) ma on na celu **usprawnienie organizacji ruchu oraz zwiększenie bezpieczeństwa na drogach**. W projekcie uczestniczą kraje Europy Środkowej i Wschodniej: Austria, Czechy, Niemcy, Polska, Słowacja, Słowenia, Węgry i Włochy. W Polsce projekt ten jest realizowany przez Instytut Badawczy Dróg i Mostów, a nadzorowany przez Generalną Dyrekcję Dróg Krajowych i Autostrad.

Już od lipca tego roku firmy Bosch Security Systems i Neurosoft testują system opracowany na potrzeby CONNECT. Dwadzieścia dwa punkty kontrolno-pomiarowe wyposażone w kamery Bosch IP (obrotowe i stałopozycyjne) oraz oświetlacze podczerwieni Extreme CCTV badają i rejestrują natężenie ruchu na głównych trasach w Polsce.

Dzięki analizie zgromadzonych danych kierowcy informowani są o utrudnieniach w ruchu, a także szacowanym czasie przejazdu na danym odcinku trasy – z uwzględnieniem natężenia ruchu, korków i zalecanych objazdów. Mierzona jest również średnia prędkość przejazdowa pojazdu na określonych trasach. Komunikat dla kierowcy o jego wykroczeniu wyświetlany jest na tablicach zmiennej treści w postaci aktualnej prędkości oraz numeru rejestracyjnego. Jednoznaczna identyfikacja pojazdów jest możliwa dzięki zastosowaniu technologii sieci neuronowych do rozpoznawania tablic rejestracyjnych. W połączeniu z nową wersją Systemu Informatycznego Schengen II (SIS II) daje to możliwość automatycznej identyfikacji skradzionych pojazdów, co wspomaga pracę policji i ułatwia odnalezienie poszukiwanego samochodu.

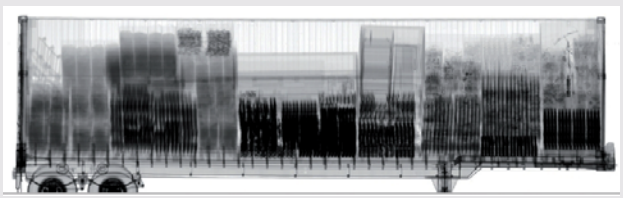
Jeżeli system opracowany na potrzeby CONNECT przejdzie testy pomyślnie, zostanie wdrożony także w pozostałych krajach Europy Środkowej i Wschodniej.

Bezpośr. inf. Emilia Dobies
Bosch Security Systems

Mobilne skanery do kontroli ładunku w polskiej Służbie Celnej

Trwa realizacja dostawy czterech **specjalistycznych pojazdów Eagle M4507 dla polskiej Służby Celnej, służących do rentgenowskiej kontroli ładunku.** Producentem urządzeń rentgenowskich, zamontowanych na podwoziu ciężarówki, jest amerykańska firma Rapiscan Systems, której autoryzowanym dystrybutorem w Polsce jest firma SAE.

Eagle M4507 to mobilny system kontroli ładunku zdolny do przemieszczania się po drogach publicznych. Jest to w pełni niezależny system, który zapewnia wszystkie elementy i możliwości wymagane do rentgenowskiego skanowania kontenerów, pojazdów i szerokiego zakresu ładunków w celu uniemożliwienia przemytu niedozwolonych lub niebezpiecznych przedmiotów, w tym broni. Dzięki zastosowaniu tego typu rozwiązań czas odprawy granicznej znacznie zmniejsza się, a skuteczność kontroli jest wysoka.



Mobilne systemy z serii Eagle Rapiscan Systems, w tym modele Eagle M4507, mogą być łatwo przewiezione z miejsca na miejsce w odpowiedzi na różne wymagania operacyjne użytkujących je służb. W ciągu 20 minut, po rozłożeniu wysięgnika w kształcie litery L, na którym zamocowana jest matryca detektorów, system jest gotowy do skanowania zaparkowanej ciężarówki bez osób w środku albo rzędu ciężarówek, zarówno w kierunku jazdy, jak i odwrotnym.

▶

Źródłem promieniowania rentgenowskiego jest akcelerator liniowy o energii 4.5 MeV. Urządzenia do obrazowania rentgenowskiego dostarczają do kabiny kontrolerów na pojeździe wysokiej jakości obrazy, które są na bieżąco oceniane przez kontrolerów przy wykorzystaniu oprogramowania **Cargo Viewer.**

System spełnia międzynarodowe i lokalne wymagania drogowe oraz standardy operacyjne, jakościowe i dotyczące bezpieczeństwa promieniowania, a jego produkcja jest zgodna ze standardami CE.

Źródło: Bezpośr. inf. SAE
Opracowanie: Adam Bułaciński, Redakcja

Spectra Mini IP – nowość z Pelco

We wrześniu do sprzedaży został wprowadzony kolejny produkt **Pelco** przeznaczony do systemów sieciowych IP – **Spectra Mini IP.** Jest to kolorowa kamera PTZ przeznaczona do pracy w pomieszczeniach o temperaturze z zakresu 0°C–50°C. Moduł kamerowy umożliwia dziesięciokrotne powiększenie optyczne i ośmiokrotne cyfrowe. W pamięci kamery mogą być zapisane 64 ujęcia, które są wybierane z dokładnością 0,5°. Maksymalna szybkość obrotowa kamery – 140°/s, a szybkość uchyłu – 80°/s.

Spectra Mini IP jest przeznaczona do instalacji nawierzchniowej lub w suficie podwieszanym. Dostępny jest opcjonalny uchwyt ścienny i wysięgnik. Obudowa może być czarna lub biała, a klosz kopuły przeźroczysty lub przyciemniony. Kamera jest przystosowana do zasilania w standardzie PoE lub napięciem zmiennym 24V.

Serwer wideo w kamerze może wysyłać strumienie wideo w formacie MPEG4 i MJPEG. Strumień MJPEG o maksymalnie 15 obrazach/s może być odbierany tylko przez przeglądarkę internetową Internet Explorer lub Mozilla Firefox. Strumienie MPEG4 o parametrach 4CIF (704x576), 25 obrazów/s mogą być odbierane przez urządzenia, które mają zaimplementowany protokół kamer IP Pelco. Takim odbiornikiem może być na przykład rejestrator hybrydowy serii DVR5100, który w wersji DVR5104 może zapisywać strumienie z szesnastu kamer IP. Na liście producentów, którzy wprowadzili protokół kamer IP Pelco, znajdują się takie firmy, jak Milestone Systems, ObjectVideo, OnSSI, Plustek, Visual Defence i Lenel Systems International.

W Polsce produkty Pelco są dostępne w sieci Partnerów firmy TAC, która jest wyłącznym przedstawicielem Pelco w Polsce. Więcej informacji o kamerze Spectra Mini IP można znaleźć na stronie www.pelco.com. Zapraszamy też na stronę www.tac.com.pl.

Bezpośr. inf. Norbert Góra, TAC

Ulisse IP

– pierwszy zintegrowany zewnętrzny zespół PTZ kontrolowany całkowicie przez IP

Videotec z dumą zapowiada opracowanie **ULISSE IP**, pierwszego zespołu PTZ do podglądu wizyjnego zapewniającego pełną integrację z systemem sieciowym. Zespół pozycjonujący obejmuje wbudowany moduł kompresji wizyjnej w celu umożliwienia sterowania IP wszystkimi funkcjami PTZ. Analogowe sygnały wizyjne i telemetryczne są konwertowane i przesyłane kablem ethernetowym w celu łatwego sterowania przy użyciu oprogramowania komputerowego.

System oferuje najwyższy współczynnik kompresji wizji przy użyciu technologii MPEG-4 dla obrazów i szybszego strumieniowania *on-line*. Maksymalna szybkość przesyłu to 30 klatek na sekundę przy maksymalnej rozdzielczości D1. Zapis odbywa się wprost na twardy dysk komputera PC. Możliwe jest podłączenie dżojstika do portu w komputerze w celu sterowania PTZ. Łatwa konfiguracja systemu jest zapewniona przez dedykowane oprogramowanie.

Zintegrowany zespół łączy zalety systemu sterowanego przez IP z wysokimi osiągami i doskonałym pozycjonowaniem niezbędnym w aplikacjach podglądowych.

ULISSE IP stworzono specjalnie do zastosowania w podglądzie wizyjnym w zewnętrznych warunkach środowiskowych, takich jak: patrolowanie wybrzeża i granic, kontrola portów, zastosowania miejskie, autostrady i monitoring ruchu drogowego, stadiony, więzienia lub obiekty wojskowe i podgląd obwodowy.

Dodatkowe informacje: www.videotec.com

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

TALOS
system ochrony granic Unii Europejskiej

2 października 2008 roku, podczas konferencji prasowej zorganizowanej przez Przemysłowy Instytut Automatyki i Pomiarów (PIAP) przy okazji wystawy „Cło i Granica 2008", nastąpiła oficjalna premiera projektu **TALOS** (ang. *Transportable, Adaptable Patrol for Land Border Surveillance System* – **Transportowalny, Adaptowalny System Patrolowania i Nadzoru Granicy Lądowej**), którego celem jest wzmocnienie bezpieczeństwa lądowej granicy zewnętrznej Unii Europejskiej, w tym jednego z najdłuższych jej odcinków, czyli wschodniej granicy Polski. Narzędziem służącym do osiągnięcia tego celu będzie szczegółowe opracowanie i wdrożenie mobilnego, autonomicznego systemu opartego o bezzałogowe platformy działające zarówno na lądzie, jak i w powietrzu, wyposażone w roboty opracowane przez PIAP.

Wprowadzenie systemu TALOS ma na celu wsparcie służb ochrony granic w wykrywaniu, śledzeniu i przechwytywaniu osób usiłujących bezprawnie przekroczyć granicę. Te założenia są zgodne z koncepcją Europejskiego Systemu Nadzoru Granic (ang. *European Surveillance System for Borders* – EUROSUR) i postanowieniami Europejskiego Zespołu Doradczego do spraw Badań nad Bezpieczeństwem (ang. *European Security Research Advisory Board* – ESRAB). Prototyp systemu TALOS zostanie zaprojektowany, zrealizowany i przetestowany w projekcie badawczym, dofinansowanym w ramach Siódmego Programu Ramowego Unii Europejskiej. Koncepcja systemu powstała w roku 2007, a projekt rozpoczął się w czerwcu br. i ma się zakończyć w roku 2012. W projekcie uczestniczy łącznie 14 partnerów – prywatnych i publicznych organizacji z obszaru przemysłu, sfery badawczo-rozwojowej oraz szkolnictwa wyższego z Belgii, Estonii, Finlandii, Francji, Grecji, Hiszpanii, Izraela, Rumunii, Turcji, a także z Polski. Zaszczytna rola koordynatora projektu przypadła **PIAP** dzięki dorobkowi tego instytutu w dziedzinie robotów antyterrorystycznych. Dwa kraje spoza Unii Europejskiej – Izrael i Turcja – uczestniczą w projekcie UE ze względu na posiadane duże doświadczenie w zakresie ochrony granic.

System opracowany w ramach przedsięwzięcia ma obejmować trzy podstawowe elementy. Należą do nich: bezzałogowe pojazdy naziemne i powietrzne, których zadaniem będzie patrolowanie granicy, naziemne wieże obserwacyjne umieszczone na platformach mobilnych oraz centrum dowodzenia zapewniające łączność pomiędzy elementami znajdującymi się w terenie a właściwą jednostką Straży Granicznej.

– TALOS jest programem pionierskim w skali światowej, bowiem nikt jeszcze nie wykorzystywał robotów w tak szerokim zakresie w równie zróżnicowanym terenie. Ze względu na liczbę uczestników jest to również znaczące wyzwanie organizacyjne – powiedział dr Jan Jabłkowski, dyrektor PIAP.

Wszystkie elementy wchodzące w skład nowego systemu są w założeniu mobilne, co umożliwi ich transportowanie i instalację w dowolnym miejscu w ciągu kilku godzin. Modularność i elastyczność systemu umożliwią szybkie dostosowanie jego parametrów do specyfiki konkretnego zadania oraz lokalnych warunków terenowych, takich jak długość odcinka granicy, ukształtowanie powierzchni czy zalesienie.

– Konwencjonalne systemy ochrony granic lądowych zbudowane są głównie z kosztownych obiektów naziemnych, rozmieszczonych wzdłuż całej granicy, które są używane do obserwacji, wykrywania i ostrzegania. Ta infrastruktura jest uzupełniana przez patrole piesze i zmotoryzowane. Dzięki nowemu, mobilnemu systemowi, usprawniającemu zarówno obserwację granicy, jak i komunikację, Straż Graniczna będzie mogła dużo szybciej reagować na zagrożenia – powiedział dr Mariusz Andrzejczak, koordynator projektu TALOS.

Zgodnie z zapowiedzią koordynatora projektu za dwa i pół roku zostanie zaprezentowana polskiej Straży Granicznej demonstracyjna wersja systemu i zostaną przeprowadzone testy w rzeczywistych warunkach w celu udowodnienia słuszności koncepcji systemu. Konsorcjum, które tworzą uczestnicy projektu, będzie prowadzić dalsze prace nad pełnym wdrożeniem systemu na europejskich granicach zewnętrznych. Będą także prowadzone prace nad integracją robotów w celu zwiększenia ich funkcjonalności.

– Chcemy rozwijać autonomiczne systemy robotyczne, ponieważ wierzymy, że staną się one w niedalekiej przyszłości ważnym elementem europejskiego systemu ochrony granic. Jesteśmy przekonani, że przyszłość konfrontacji z niebezpieczeństwem to roboty – podsumował dr Jabłkowski.

Opracował: Adam Bułaciński, Redakcja
Źródło: prezentacje PIAP
oraz materiały prasowe agencji
Solski Burson-Marsteller

XI Seminarium
Forum Monitoringu Polskiego – relacja

W dniach 2 i 3 października 2008 roku odbyło się **XI Seminarium Forum Monitoringu Polskiego** organizowane przez **Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm”**. Tegoroczna impreza odbyła się w Centrum Szkoleń i Konferencji „Geovita” w Jadwisinie, które położone jest nad samym brzegiem Zalewu Zegrzyńskiego. Malownicza okolica stworzyła klimat zarówno do pracy, jak i odpoczynku, a organizatorzy imprezy mogą pochwalić się dużym zainteresowaniem ze strony uczestników.

W tym roku forum było podzielone na trzy panele tematyczne:

1. zagadnienia prawno-organizacyjne wpływające na efektywność biznesową SMA;
2. zagadnienia techniczne w monitoringu alarmowym obiektów stacjonarnych i ruchomych;
3. zagadnienia techniczne w monitoringu wizyjnym.

Dr inż. Andrzej Ryczer i mgr inż. Krzysztof Ciesielski, który w tym roku pełnił rolę koordynatora merytorycznego forum, powitali gości i omówili program seminarium.

Podczas pierwszego panelu uczestnicy mogli wysłuchać m.in. prezentacji dr inż. Jerzego Pawlika na temat aktualnych wymagań KG Policji dotyczących zabezpieczenia Stacji Monitorowania Alarmów oraz wyposażenia operatorów stacji monitorowania w broń palną w oparciu o plan ochrony. W kolejnych wystąpieniach omówiono problemy związane z ochroną danych osobowych oraz doświadczenia praktyczne we wdrażaniu systemów zarządzania bezpieczeństwem informacji, które przedstawił słuchaczom dr inż. Andrzej Wójcik. Na temat systemu zarządzania bezpieczeństwem w bankach wypowiedzieli się mgr inż. Andrzej Starnawski i mgr inż. Krzysztof Białek. Prowadzenie wspólnej polityki bezpieczeństwa fizycznego i IT, standaryzacja systemów bezpieczeństwa i umów z podmiotami zewnętrznymi to jedne z ważniejszych składowych systemu zarządzania bezpieczeństwem w bankach. Te elementy przyczyniają się nie tylko do ulepszenia systemu bezpieczeństwa informacji, czy też gotówki, ale przede wszystkim do zwiększenia bezpieczeństwa ludzi.

Drugi panel seminarium otworzył dr inż. Andrzej Ryczer. Wygłosił on wykład pt. „Wymagania projektu Normy Europejskiej prEN50118-1:2008 Centrum monitoringu i odbioru alarmu – Część 1: Wymagania dotyczące lokalizacji i konstrukcji. Zastosowanie do oceny bezpieczeństwa fizycznego alarmowego centrum odbiorczego ACO". Porównanie stanu polskich Stacji Monitorowania Alarmów ze standardami przyjętymi w innych krajach przedstawił mgr inż. Daniel Kamiński. Warto wziąć pod uwagę to, że przy wprowadzaniu nowych rozwiązań musimy zawsze pamiętać o potrzebach klienta, które są coraz większe. O niezawodności systemu informatycznego mówił mgr inż. Piotr Małecki z firmy AD INFO.

Panel trzeci składał się z prezentacji firm, które oferują produkty do monitoringu wizyjnego. O wysokiej rozdzielczości sieciowych kamerach IP Mobotix mówił Witold Faber z firmy Linc. Dr Kazimierz Bulandra, prezes zarządu firmy KABE, przedstawił nowoczesne systemy radarowo-kamerowe, zasady ich funkcjonowania oraz zalety wynikające z ich zastosowania. Podczas tego panelu pojawiła się również prezentacja firmy Wincor-Nixdorf. Mgr inż. Jakub Wnuk przedstawił sposoby walki z coraz bardziej popularnym w naszym kraju zjawiskiem skimmingu, czyli kopiowaniem paska magnetycznego karty, którą wykorzystujemy w bankomacie. Dodatkową atrakcją dla uczestników

„Nowoczesny system monitorowania oraz nowe podejście do aspektów monitoringu klientów indywidualnych" to tytuł kolejnej prezentacji, a prelegentem był mgr inż. Daniel Kossman z firmy Qitio. Ostatnia prezentacja w tym panelu należała do firmy Gorke. Pierwszy dzień forum zakończył się kolacją i doskonałą zabawą w kasynie.

Drugi dzień seminarium, a także ciąg dalszy drugiego panelu tematycznego, rozpoczął się od wykładu pt. „Charakterystyka systemów GPS do monitorowania obiektów i osób" firmy Kera-

była możliwość zapoznania się z wnętrzem bankomatu, który został przywieziony przez przedstawicieli firmy Wincor-Nixdorf. Mamy nadzieję, że możliwość poznania mechanizmów działania bankomatu, a tym samym sytuacji sprzyjających skimmingowi, przyczyni się do powstania lepszych zabezpieczeń tych urządzeń, z których korzystają miliony Polaków. Na zakończenie trzeciego panelu tematycznego, a tym samym na zakończenie seminarium, odbyło się podsumowanie i rozdanie zaświadczeń potwierdzających uczestnictwo w seminarium.

tronik. Ostatnia prezentacja w tym panelu należała do mgr inż. Krzysztofa Ciesielskiego. Brak sygnału GPRS to bardzo duży problem dla stacji monitorowania alarmów. Ostatni wykład podczas tego panelu, podobnie jak wcześniejsze wystąpienia oraz dyskusja moderowana z prelegentami, z pewnością pozwolił słuchaczom wyciągnąć odpowiednie wnioski dotyczące mo-

W imieniu redakcji czasopisma *Zabezpieczenia* bardzo dziękujemy za zaproszenie i możliwość wzięcia udziału w XI Seminarium Forum Monitoringu Polskiego.

Do zobaczenia za rok...

Ela Końka, Redakcja

Alarm 2008

relacja

W dniach 5–6 listopada 2008 roku w kieleckim ośrodku wystawienniczym odbyła się **Międzynarodowa Konferencja „Bezpieczny Stadion”** i towarzysząca jej wystawa **„Alarm, Sport-Obiekt”** oraz **Ogólnopolska Konferencja „Bezpieczne Miasto” – Monitoring wizyjny miast.** Jednym z celów konferencji było stworzenie forum wymiany doświadczeń związanych z systemami monitoringu wizyjnego.

Honorowy patronat nad wystawą objęli minister spraw wewnętrznych i administracji Grzegorz Schetyna, minister sportu Mirosław Drzewiecki, I zastępca komendanta głównego policji nadins. Arkadiusz Pawełczyk oraz Polski Komitet Olimpijski.

Przybyłych gości i uczestników obu konferencji powitał prezes zarządu Targów Kielce – dr Andrzej Machoń, natomiast sprawami organizacyjnymi zajął się, jak co roku, dyrektor wystawy i konferencji Grzegorz Figarski.

Konferencja „Bezpieczny Stadion”, której współorganizatorem był Polski Związek Piłki Nożnej, jest nie tylko elementem ogólnonarodowej kampanii na rzecz poprawy bezpieczeństwa, a także modernizacji, podniesienia poziomu estetyki i komfortu w obiektach sportowych, ale również okazją do wymiany doświadczeń i informacji dla specjalistów z dziedziny zabezpieczeń (zarówno technicznych, jak i fizycznych), przedstawicieli klubów sportowych (zarówno krajowych, jak i zagranicznych), a także przedstawicieli przedsiębiorstw pracujących na rzecz poprawy bezpieczeństwa oraz budowy i modernizacji obiektów sportowych. Wśród zaproszonych gości była przedstawicielka Ministerstwa Spraw Wewnętrznych i Administracji, Grzegorz Lato – nowo wybrany prezes PZPN, Adam Olkowicz – wiceprezes PZPN ds. EURO 2012, Borys Voskresensky – wiceprezydent Federacji Futbolu Ukrainy oraz przedstawiciele policji z Niemiec.

Adam Olkowicz, podobnie jak rok temu, przedstawił aktualny stan przygotowań do EURO 2012.

Przedstawicielka MSWiA poinformowała uczestników konferencji o nowelizacji aktualnie obowiązującej ustawy o bezpieczeństwie imprez masowych, a także o tym, że wicepremier i minister spraw wewnętrznych i administracji został przez premiera wyznaczony na jednego z dwóch wiceprzewodniczących komitetu organizacyjnego EURO 2012. Jako organ pomocniczy ministra powołano zespół ds. koordynacji działań służb podległych MSWiA w związku z organizacją EURO. Przewodniczącym zespołu resortowego został podsekretarz stanu w MSWiA minister Adam Rapacki. W skład zespołu wchodzą szefowie służb: policji, Straży Granicznej, Państwowej Straży Pożarnej, BOR-u, dyrektorzy poszczególnych komórek ministerstwa, które będą bezpośrednio zaangażowane w trakcie EURO.

Borys Voskresensky przedstawił w swoim wystąpieniu zagadnienia dotyczące bezpieczeństwa na stadionach piłkarskich na Ukrainie przy przygotowywaniu i w trakcie trwania mistrzostw europy w piłce nożnej.

Liczni przedstawiciele policji niemieckiej, opierając się na swoich doświadczeniach, przekazali słuchaczom refleksje dotyczące bezpieczeństwa na stadionach w kontekście ścisłej współpracy organizatorów imprez sportowych z policją, a także przedstawili wymagania UEFA i FIFA w stosunku do stadionów, na których są rozgrywane międzynarodowe mecze piłkarskie (na przykładzie Monachium i Norymbergii).

Ireneusz Troszczyński, naczelnik Wydziału Bezpieczeństwa Przewozów „PKP Przewozy Regionalne”, omówił działania PKP na rzecz zapewnienia bezpieczeństwa w pociągach podczas przejazdu grup kibiców sportowych.

Na zakończenie pierwszego dnia odbyła się uroczysta **Gala Fair Play**, podczas której zostały wręczone puchary i wyróżnienia Prezesa PZPN za wzorową organizację za-

wodów i zapewnienie bezpieczeństwa uczestnikom oraz kulturalne zachowanie publiczności na zawodach piłki nożnej i zawodach sportowych w sezonie 2007/2008.

Z przyjemnością informuję, że z naszej branży **w kategorii „Alarm" Medale Targów Kielce otrzymali:**

1. **ISM Eurocenter** za SECURE – M oraz innowacyjne podejście do integracji systemów bezpieczeństwa. Firma ISM Eurocenter powstała w połowie 2008 roku. Zajmuje się wprowadzeniem na polski rynek zaawansowanych technologicznie systemów do inteligentnego zarządzania bezpieczeństwem fizycznym i technicznym. Oferowane systemy są oparte na tworzonych indywidualnie, dobieranych do potrzeb klienta, rozwiązaniach łączących zarówno nowoczesne, jak i tradycyjne zabezpieczenia w sprawne i skuteczne narzędzia zarządzania środkami ochrony technicznej.
2. **GV Polska** za cyfrowy rejestrator 32-kanałowy QUADRUPLEX – nowoczesny system rejestracji obrazu.

Wyróżnienia Targów Kielce otrzymali:

1. **Miwi-Urmet** za system IndigoVision. System IndigoVision to wysokiej jakości system IP posiadający cechy tradycyjnych systemów CCTV, takie jak: zapis na rejestratorach autonomicznych, funkcje krosownicy, możliwość podłączania analogowych monitorów, zarządzanie funkcjami wyświetlania oraz sterowania PTZ za pomocą sprzętowego sterownika z dżojstikiem. System charakteryzuje się bardzo wysoką jakością obrazu przy zachowaniu stosunkowo małych strumieni danych. Dedykowany jest zarówno do małych instalacji wykorzystujących infrastrukturę sieci komputerowej, w tym również sieci bezprzewodowej (np. monitoringu w małych miastach, monitoringu firm, osiedli), jak również dużych systemów instalowanych w portach lotniczych, na stadionach, autostradach czy w dużych wielotysięcznych miastach).
1. **Dipol** za Ultisystem (oprogramowanie pozwalające na współpracę lokalnych systemów monitoringu z monitoringiem miejskim).

W imieniu całej redakcji wszystkim nagrodzonym serdecznie gratuluję.

Udział w targach Sport-Obiekt i Alarm wzięło 65 wystawców z Polski, Wielkiej Brytanii, Turcji i Austrii (w tym 12 firm z naszej branży). Wystawcy zaprezentowali nowe trendy w budownictwie sportowym oraz kompleksową ofertę wyposażenia obiektów sportowych, a także sprzęt sportowo-rekreacyjny.

Firma Trias z Torunia zaprezentowała między innymi najnowocześniejszy, olbrzymi mobilny telebim o powierzchni 50 m^2 z możliwością obracania się w trakcie imprezy (np. podczas mistrzostw świata w piłce nożnej) o prawie 360°. Montaż i demontaż trwa zaledwie pół godziny.

Nasza branża (security) reprezentowana była przez następujące przedsiębiorstwa:

3D, Dipol, Fortuna Communication, Gastop, Gunnebo Polska, GV Polska, ISM EuroCenter, Miwi-Urmet, NsyTech, Radioton, Transcom System oraz organizację zrzeszającą firmy branży zabezpieczeń prowadzące działalność handlową i produkcyjną oraz świadczące usługi projektowania i instalacji systemów zabezpieczeń technicznych **– Polską Izbę Systemów Alarmowych.**

Konferencja „Bezpieczne Miasto" tradycyjnie, zgodnie z założeniem, poświęcona była monitoringowi wizyjnemu miast (tych dużych i tych mniejszych), osiedli, szkół, autobusów, a także obiektów sakralnych.

Ciekawy referat wygłosiła Małgorzata Muzoł – świętokrzyski kurator oświaty. Tematem był wpływ monitoringu wizyjnego na poprawę bezpieczeństwa w szkołach na przykładzie województwa świętokrzyskiego. Małgorzata Muzoł omówiła między innymi ankietę, która

została przeprowadzona w tym województwie. Wynika z niej, że zdecydowana większość respondentów (107 spośród 112 ankietowanych dyrektorów szkół) uważa, że system monitoringu ma duży wpływ na poprawę bezpieczeństwa w placówkach oświatowych, przyczynia się do wykrywania sprawców kradzieży, aktów wandalizmu, monitoruje obecność obcych osób na terenie szkoły i w jej pobliżu. Jak twierdzi prelegentka, zamontowanie kamer pozwoliło zdyscyplinować zarówno młodzież, jak i nauczycieli. Zapewniła, że w roku 2009 projekt „Bezpieczna i przyjazna szkoła" będzie kontynuowany. Tę opinię potwierdził również Kazimierz Mądzik – kolejny prelegent – dyrektor Zespołu Szkół Informatycznych w Kielcach. Słuchacze mieli okazję zajrzeć na parę minut za pomocą łączy internetowych do ZSI, aby przekonać się, jak działają zainstalowane tam kamery, a także zapoznać się ze sposobem zapisu i archiwizacji nagrań.

Referat „Megapikselowy przewrót w monitoringu miejskim" wygłosił Maciej Włodarczyk z firmy Dipol, a Tomasz Kruszyński z Miwi-Urmetu zaprezentował słuchaczom IndigoVision – system bezpieczeństwa Video IP, który może być zastosowany między innymi w monitoringu miejskim.

Marek Wołoch – prezes zarządu Przedsiębiorstwa Komunikacji Miejskiej – przedstawił natomiast wyniki testowania systemów monitoringu w autobusach miejskich w Kielcach i omówił ich wpływ na bezpieczeństwo.

Georgis Bogdanis zademonstrował pokazane już wcześniej na targach Securex 2008 bezzałogowe urządzenie latające, które może być wykorzystane jako nośnik urządzeń wizyjnych.

Dwa kolejne referaty dotyczyły zabezpieczenia i monitoringu zabytkowych kościołów oraz aspektów organizacyjnych, czyli odpowiedniego rozpoznawania obiektu, wykonywania dokładnego projektu obiektu, znajdowania najsłabszych punktów, wyeliminowania ich (np. przez usunięcie wysokich drzew, krzewów, usunięcie przedmiotów mogących posłużyć za drabinę itp.). Referaty wygłosili kolejno: nadkom. Tomasz Malinowski z Wydziału Transportu KWP w Krakowie oraz ks. Paweł Tkaczyk – konserwator diecezjalny w Kielcach.

Ostatnie trzy referaty to:

1. „Aspekty projektowania pojazdów specjalnych policji" – nadkom. Tomasz Malinowski, asp. Robert Piowar z Wydziału Transportu KWP w Krakowie.
2. „Nowoczesne systemy monitoringu wizyjnego w Starachowicach" – podins. Grzegorz Makuch – z-ca komendanta KPP w Starachowicach. Dziesięć kamer stacjonarnych i jedna mobilna strzeże bezpieczeństwa w mieście. Do końca listopada ma być sześć kolejnych. Docelowo system miejskiego monitoringu w Starachowicach ma liczyć 25 kamer. 24 września br. w Komendzie Powiatowej Policji odbył się oficjalny odbiór systemu monitoringu wizyjnego. System będzie pracował przez całą dobę, a obsługiwać go będą emerytowani policjanci.
3. „System monitoringu miejskiego w Połańcu" – Ernest Gałek – zastępca burmistrza miasta i gminy Połaniec. Stworzenie sieci monitorowania miasta to wspólna inicjatywa władz samorządowych Połańca oraz policji.

Na koniec moja osobista refleksja. Spotkałam się ze skrajnie różnymi opiniami na temat monitoringu wizyjnego miast. Często stanowiska te opierały się na przeprowadzonych badaniach. Nie czuję się upoważniona do oceny przeprowadzonych ankiet i badań ani formułowania opinii na temat słuszności czy bezzasadności instalacji systemów monitoringu. Wiem jedno – lepiej robić cokolwiek niż nie robić nic.

Zapraszamy do oberzenia fotogalerii z konferencji na www.zabezpieczenia.com.pl

Teresa Karczmarzyk

Relacja z jubileuszowej, trzydziestej edycji targów BEZPEKA

W dniach 21–24 października br. w centrum wystawienniczym Kiev Expo Plaza miały miejsce targi elektronicznych systemów zabezpieczeń „Systemy i środki bezpieczeństwa". Była to jubileuszowa, trzydziesta edycja targów popularnie nazywanych „Bezpeka".

Targi zasłużenie cieszą się opinią największych i najbardziej prestiżowych targów elektronicznych systemów bezpieczeństwa na Ukrainie.

O randze wydarzenia świadczy m.in. długa lista osób oficjalnie otwierających targi z zastępcą ministra d/s sytuacji nadzwyczajnych czy zastępcą przewodniczącego Narodowej Akademii Nauk Ukrainy. Na targach swoje osiągnięcia prezentowało również wiele instytucji państwowych, m.in. Państwowa Służba Ochrony przy Ministerstwie Spraw Wewnętrznych, Państwowy Instytut Naukowo-Badawczy Ministerstwa Spraw Wewnętrznych Ukrainy, Służba Bezpieczeństwa Ukrainy, Państwowa Służba Łączności Specjalnej i Ochrony Informacji, Państwowa Służba Celna Ukrainy, Centrum Konstrukcyjno-Technologiczne Ministerstwa Obrony Ukrainy.

Tegoroczna edycja targów wielkością odpowiada dwóm poprzednim. Świadczy o tym chociażby wykupiona powierzchnia wystawiennicza 3600 m2, porównywalna z edycją Bezpeka 2007. Aranżacja standów, ich wielkość oraz przemyślana koncepcja wyróżniały się na tle poprzednich edycji. Choć organizatorzy targów nie podali jeszcze oficjalnych danych liczby osób odwiedzających targi, to własne obserwacje wskazują na to, że ich liczba była podobna, jak w roku ubiegłym.

W targach uczestniczyło 196 wystawców z Ukrainy, Polski, Rosji, Słowacji, Finlandii, Hiszpanii oraz tradycyjnie z Korei Południowej, będącej jednym z największych eksporterów elektronicznych systemów zabezpieczeń. Dominowały firmy i brandy, które zadomowiły się już na lokalnym rynku, natomiast niewiele było firm po raz pierwszy wystawiających się na targach. Świadczyć to może o dojrzałości tamtejszego rynku sytemu zabezpieczeń.

Targi odbyły się w samym szczycie światowego kryzysu gospodarczego, który szczególnie mocno odczuła również Ukraina. W trakcie całotygodniowego pobytu w Kijowie w czasie targów doszło do dwudziestoprocentowego osłabienia ukraińskiej waluty w stosunku do dolara, co było częstym tematem rozmów. Nie może to dziwić w sytuacji, gdy główną walutą importu dalekowschodniego sprzętu ciągle pozostaje amerykański dolar. Ten szczególny czas trwania targów mógł mieć wpływ na liczbę zwiedzających.

Targi Bezpeka odbywają się w cyklu rocznym. Kraj pochodzenia uczestników wyraźnie wskazuje na wybitnie krajowy charakter wydarzenia. Należy mieć nadzieję, że targi będą w dalszym ciągu dynamicznie się rozwijać, czego życzymy organizatorom.

Do zobaczenia na targach Bezpeka 2009.

Bezpośr. inf. Redakcja

Wpływ akustyki wnętrza na efektywność Dźwiękowego Systemu Ostrzegawczego – relacja z konferencji firmy Ambient System

22 października 2008 roku w warszawskim hotelu Sofitel Victoria odbyła się bezpłatna naukowo-techniczna **konferencja szkoleniowa**, zorganizowana przez firmę **Ambient System** – dystrybutora i projektanta systemów obiektowych: nagłośnieniowych, pożarowych i komunikacyjnych. Tytuł tegorocznej konferencji brzmiał: **„Wpływ akustyki wnętrza na efektywność Dźwiękowego Systemu Ostrzegawczego”**. W konferencji wzięło udział kilkadziesiąt osób, głównie projektanci oraz wykonawcy systemów DSO i SSP oraz systemów wentylacji.

Konferencja została zorganizowana wspólnie z trzema innymi firmami zajmującymi się pokrewną działalnością:

- **Fläkt Bovent** (dostawca systemów klimatyzacji i wentylacji, w tym strumieniowej),
- **Pimco Acoustics** (wykonawca usług w zakresie szeroko rozumianej akustyki architektonicznej),
- **Wibroakustyka** (dostawca innowacyjnych rozwiązań służących do zwalczania drgań i hałasu).

Oprócz przedstawicieli ww. czterech firm w gronie autorów przedstawionych referatów znaleźli się zaproszeni goście z **Instytutu Techniki Budowlanej** (ITB). Czasopismo ***Zabezpieczenia*** było patronem medialnym imprezy.

Organizatorzy konferencji prezentowali swoją ofertę na rozstawionych w sali obrad stoiskach. Duże zainteresowanie wzbudziły urządzenia dźwiękowego systemu ostrzegawczego **ABT-Venas** (wcześniej znanego jako **MCR-Venas**) firmy Ambient System, w tym sporych rozmiarów **głośnik dalekiego zasięgu z serii ABT-K**, stosowany zarówno w DSO, jak i do nagłaśniania stadionów.

Otwarcia konferencji dokonał prezes zarządu Ambient Systems – **Piotr Szaliński**, który omówił strategię i dokonania swojej firmy, wspominając m.in. o unikatowej konstrukcji **mikrofonu strażaka** w systemie ABT-Venas, umożliwiającej bardzo duże zbliżenie do ust mówiącego (*close-up*). Następnie, w trzech sesjach przedzielonych przerwami, zaprezentowano osiem referatów wymienionych poniżej.

1. Zjawiska akustyczne w pomieszczeniach i ich wpływ na zrozumiałość mowy – **Elżbieta Nowicka**, ITB;
2. Uwzględnienie akustyki wnętrza w procesie projektowania DSO – **Leszek Demidowicz**, Ambient System;
3. Eliminacja hałasu pogłosowego przy pomocy natryskowych, celulozowych tynków dźwiękochłonnych – **Wiesław Fiebig**, Wibroakustyka;
4. Nowości na rynku DSO – Leszek Demidowicz, Ambient System;
5. Praktyczne sposoby kształtowania współczynnika zrozumiałości mowy – Leszek Demidowicz, Ambient System;
6. Rozwiązania ograniczające hałas od elementów systemu oddymiania strumieniowego Jet-Thrust – **Włodzimierz Łącki**, Fläkt Bovent;

7. Istotne wymagania, jakie musi spełnić DSO w świetle aktualnych przepisów – **Jerzy Ciszewski**, ITB;
8. Redukowanie czasu pogłosu poprzez zastosowanie absorberów – **Michał Kamiński**, Pimco Acoustics.

W jednym ze swoich wystąpień Leszek Demidowicz poinformował o uzyskaniu **nowego certyfikatu zgodności** oraz **świadectwa dopuszczenia CNBOP** dla oferowanego przez Ambient System systemu ABT-Venas. Zapowiedział także wejście na rynek na początku roku 2009 **nowych serii głośników – ABT-S** (sufitowych) oraz **ABT-T** (tubowych), które aktualnie są poddawane badaniom w CNBOP. Stanie się wtedy dostępny pełen asortyment głośników tubowych, które będą mogły być stosowane tam, gdzie dotychczas używano projektorów dźwięku, w zastosowaniach, w których nie jest wymagana wysoka jakość dźwięku (przy niższej cenie takiego rozwiązania). Wysoką jakość dźwięku zapewnią nowe konstrukcje głośników umieszczonych w kolumnach, które „chętnie miałby z pewnością w swoim DSO każdy jego użytkownik", jak powiedział Leszek Demidowicz.

Z wielu referatów można było dowiedzieć się interesujących informacji na temat podstaw fizycznych dźwięku oraz akustyki. Można było także usłyszeć niekorzystne zjawiska dźwiękowe, jakie powstają w warunkach niewłaściwej akustyki pomieszczeń (np. pogłos, echo trzepoczące) oraz efekty zastosowania rozwiązań służących do ich ograniczenia lub eliminacji.

Do podstawowych problemów, z jakimi borykają się projektanci i wykonawcy DSO, należy negatywny wpływ na słyszalność komunikatów DSO innych systemów obiektowych działających w tych samych pomieszczeniach oraz powszechne zjawisko nieuwzględniania podstawowych zasad akustyki w projektach architektonicznych, w których liczy się zwykle robiący wrażenie końcowy efekt wizualny, co nie zawsze (zazwyczaj rzadko) idzie w parze z przydatnością pomieszczeń do odsłuchiwania dźwięku. Wpływ innych systemów można wyeliminować przez koordynację działań projektowych i realizacyjnych w ujęciu całościowym, nie ograniczającym się do poszczególnych systemów, ale uwzględniającym współdziałanie wszystkich systemów, które mają ze sobą współistnieć w obiekcie. Pozwala to na wybór właściwych, a nie przypadkowych rozwiązań. Jedynym zaś rozwiązaniem umożliwiającym prawidłowe działanie DSO w warunkach niewłaściwej akustyki pomieszczeń jest w wielu przypadkach zastosowanie produktów oferowanych np. przez firmy Pimco Acoustics (różnego rodzaju tzw. ustrojów – pochłaniających, odbijających, rozpraszających i kombinowanych, których wielokolorowe próbki uczestnicy konferencji mieli okazję obejrzeć podczas prezentacji Michała Kamińskiego) lub Wibroakustyka (tynków dźwiękochłonnych celulozowych, nanoszonych na różnego rodzaju podłoża natryskowo, przydatnych nawet w przypadku powierzchni o nieregularnych kształtach; także innych materiałów dźwiękochłonnych i dźwiękoizolacyjnych).

W trakcie wielu wystąpień zadawano pytania z sali oraz wygłaszano komentarze. Na zakończenie głos ponownie zabrał Leszek Demidowicz, wyrażając nadzieję, że podczas następnej konferencji firmy Ambient System, która ma być zorganizowana w **maju 2009 roku**, będzie można porozmawiać więcej o rozwiązaniach problemów, a nie tylko o ich istnieniu. Prezes Szaliński zaprosił następnie wszystkich uczestników konferencji na obiad w hotelowej Restauracji Hetmańskiej, gdzie można było kontynuować rozpoczęte podczas konferencji dyskusje.

Adam Bułaciński, Redakcja

Rekordowe targi SECURITY 2008 w Essen (podsumowanie)

Targi **SECURITY 2008**, które odbyły się w Essen (Niemcy) w dn. **od 7 do 10 października 2008 r.** i dotyczyły **zabezpieczeń** oraz **ochrony przeciwpożarowej**, odwiedziła **rekordowa liczba zwiedzających: 40850 osób**, a 32.3% stanowili wśród nich przybysze ze 115 krajów świata, głównie z Europy, a poza tym z Azji i Ameryki. Miarą międzynarodowego sukcesu jest też liczba wystawców – spośród **1100 wystawców**, którzy prezentowali swoje produkty i usługi, aż 480 pochodziło z zagranicy, z 42 krajów. Zaobserwowano duże zainteresowanie gości technologiami **dozoru wizyjnego, kontrolą dostępu i zabezpieczeniami przeciwpożarowymi.**

– *Targi Security dowiodły w robiący wrażenie sposób swojej pozycji jako numeru 1 na świecie w tej branży* – stwierdził **Egon Galinnis**, Dyrektor Zarządzający Targów w Essen *(Messe Essen)*. Rozległy zakres oferty targowej przyciągnął do Essen czołowych decydentów z zakresu systemów bezpieczeństwa, którzy stanowili aż 63.6% gości. – *Wielu wystawców poinformowało o zawarciu podczas targów znaczących kontraktów.*

Sukcesem okazała się premiera wydzielonej **Hali 12 poświęconej wyłącznie ochronie przeciwpożarowej.** – *Nie słyszałem, aby którykolwiek z wystawców w Hali 12 nie chciał się tu pojawić następnym razem. Będziemy wtedy potrzebować nawet jeszcze większej powierzchni niż teraz* – powiedział dr **Wolfram Krause**, Dyrektor Zarządzający Bundesverband Technischer Brandschutz (Federalnego Związku Technicznej Ochrony Przeciwpożarowej). Głównym punktem programu był zorganizowany 9 października **Dzień Ochrony Przeciwpożarowej**, w którym miało miejsce najwięcej pokazów, w tym w wykonaniu straży pożarnej z Essen, a także odbywały się dyskusje podczas otwartego forum w Hali 12.

We wszystkich sekcjach targów goście mieli okazję do zapoznania się z **licznymi innowacjami, a nawet premierami światowymi**. Zaprezentowano na przykład nowe możliwości telewizji dozorowej, wykorzystujące ulepszoną technologię kamer, systemy kontroli dostępu z rozpoznawaniem układu naczyń krwionośnych dłoni czy niewielkich rozmiarów detektory dymu. Po raz pierwszy **innowacje zostały uhonorowane nagrodami** *(Security Innovation Awards)*. W kategorii „Produkty i technologia" złoty medal przyznano firmie **Kaba** za **bezkontaktowy system kontroli dostępu typu *„touch go"*** („dotknij i przejdź" – przyp. redakcji), srebrny firmie **Observision** za **Videominer** – rozwiązanie pozwalające na **szybką ocenę materiału wizyjnego**, a brązowy firmie **PCS Systemtechnik** za **IntusPalm Secure** – system **rozpoznawania układu naczyń krwionośnych dłoni.**

Otwarte fora zaoferowały ponad 160 wykładów, dyskusji okrągłego stołu i pokazów. Mówcy w Hali 4 zwracali uwagę na **niebezpieczeństwa, jakie czyhają w Internecie.** Forum w Hali 12 skupiło się na **zarządzaniu bezpieczeństwem i ochronie przeciwpożarowej.** Atrakcją targów stała się możliwość zapoznania się z pracą **zespołów pracujących z psami** – wąchającymi i obronnymi. Przez dwa dni odbywał się, w nowej formule, kongres „Bezpieczeństwo w dialogu" – wtorek był poświęcony badaniom bezpieczeństwa cywilnego, a imprezy środowe miały nazwę **„Utrata know-how: małe i średnie przedsiębiorstwa jako cele ataku".**

Mimo obecnego kryzysu finansowego branża zabezpieczeń patrzy w przyszłość optymistycznie. Na całym świecie zanotowano w tej branży wzrost obrotów rzędu 3–4%. Ponad 60% gości oceniło sytuację ekonomiczną swoich firm jako bardzo dobrą.

Następne targi **SECURITY w Essen** odbędą się w dniach od **5 do 8 października 2010 r.**, ale już za rok nastąpi **rosyjska premiera targów – SECURITY Russia w Moskwie (27–30 października 2009 r.).**

Bezpośr. inf. Messe Essen
Opracowanie: Adam Bułaciński, Redakcja

Firma HID Global bawiła się w Cambridge

Wspaniałe otoczenie Queens' College w Cambridge zapewniło niezapomniane wrażenia uczestnikom imprezy zorganizowanej przez uznanego **lidera w dziedzinie rozwiązań bezpiecznej tożsamości – firmę HID Global** w tym historycznym miejscu o 550-letniej tradycji. Klienci i partnerzy regionu EMEA HID Global, obejmującego Europę, Bliski Wschód i Afrykę, a także przedstawiciele prasy mieli okazję nie tylko poznać nowego szefa regionu, ale i wziąć udział w **prezentacji na temat przyszłych technologii w wykonaniu Davida Bodanisa, autora książki E=mc²**, czyli historii najsłynniejszego równania świata.

Goście obejrzeli także **nową siedzibę HID Global EMEA w Haverhill**, gdzie szef regionu EMEA **Paul Naldrett** nakreślił plany strategicznego rozwoju kierowanego przez siebie przedsiębiorstwa. Oprócz najnowszych informacji o wzmocnieniu portfolio firmy dzięki ostatnio dokonanym przejęciom i o tym, jak technologia HID i takie produkty, jak **SmartID** i **OMNIKEY** są wykorzystywane w każdej dziedzinie gospodarki – od szpitali po elektroniczną administrację (ang. *E-government*), od handlu po edukację, jedną z najważniejszych dyskutowanych spraw była pionierska rola, jaką pełni HID w konwergencji fizycznych i logicznych systemów dostępowych. Przykładem takiej konwergencji może być wyposażanie nowych laptopów Dell Latitude w czytniki iClass firmy HID, co zostało ogłoszone podczas spotkania. Taka technologia nie tylko zapobiega uzyskaniu nieautoryzowanego dostępu do laptopa i zgromadzonych w nim danych, ale i umożliwia używanie jednej karty HID iClass zarówno do fizycznej kontroli dostępu w budynku, jak i w celu bezpiecznego logowania się do komputera.

Więcej na ten (i nie tylko) temat można było usłyszeć podczas targów CARTES & IDentification, które odbyły się w Paryżu.

Źródło: Bezpośr. inf. HID Global
Opracowanie: Adam Bułaciński, Redakcja

CŁO i GRANICA 2008
– podsumowanie

XIV Międzynarodowa Wystawa **Wyposażenia dla Kontroli Celnej i Granicznej „CŁO i GRANICA”** została zorganizowana w Hotelu Gromada – Centrum Kongresowo-Wystawienniczym w Warszawie, w dniach 1 i 2 października 2008 roku. Współorganizatorem wystawy była Polska Izba Producentów na Rzecz Obronności Kraju, a patronami honorowymi – Szef Służby Celnej oraz Komendant Główny Straży Granicznej.

W gronie 29 wystawców znaleźli się m.in. producenci i dystrybutorzy produktów przeznaczonych dla służb kontroli celnej i granicznej, a także dla straży ochrony kolei – począwszy od umundurowania, broni i innego wyposażenia osobistego przez środki służące do usuwania substancji niebezpiecznych po różnego rodzaju sprzęt, w tym służący do **podniesienia efektywności kontroli i zwiększenia bezpieczeństwa osób.** Wśród tego sprzętu warto wymienić np. lornetki i kamery termowizyjne, wideoendoskopy oraz

inne urządzenia służące do kontroli wizualnej, detektory metali, narkotyków, materiałów wybuchowych, gazów niebezpiecznych itp., rentgenowskie skanery do sprawdzania bagażu oraz ładunku czy antyterrorystyczne roboty mobilne.

Pierwszego dnia wystawy odbyła się także **konferencja „Program ochrony granic Polski i UE – plany, rozwiązania, innowacje”**, składająca się z pięciu sesji tematycznych. Jedna z nich była poświęcona innowacyjnym sprzętowym rozwiązaniom dla służby celnej i straży granicznej. Konferencję zakończyła sesja na temat **zagrożeń terrorystycznych** i walki z nimi.

Podczas drugiego dnia wystawy odbyła się konferencja prasowa jednego z wystawców – Przemysłowego Instytutu Automatyki i Pomiarów, prezentującego unijny projekt TALOS, związany z **patrolowaniem i nadzorem granic lądowych**, przewidujący wykorzystanie wspomnianych wyżej robotów mobilnych.

Wystawa i konferencja zgromadziły z jednej strony grono odbiorców i użytkowników, a z drugiej – dostawców wysoce specjalistycznych rozwiązań, stwarzając okazję do bezpośrednich rozmów na tematy nurtujące uczestników tej połączonej imprezy, wzbogaconą o możliwości wynikające z bezpośredniego kontaktu z prezentowanymi na stoiskach produktami.

Adam Bułaciński, Redakcja

„Bezpieczeństwo – wymiar współczesny oraz perspektywy badań”

Relacja z konferencji

W dniach 12 i 13 października 2008 roku w kampusie **Krakowskiej Szkoły Wyższej** im. Andrzeja Frycza Modrzewskiego odbyła się **międzynarodowa konferencja naukowa pt. „Bezpieczeństwo – wymiar współczesny oraz perspektywy badań”**. W ciągu ośmiu lat istnienia uczelnię im. Andrzeja Frycza Modrzewskiego ukończyło 18 tys. studentów, co stawia ją na drugim miejscu wśród największych uczelni niepublicznych w Polsce. Od niedawna można na niej studiować także – na **Wydziale Nauk o Bezpieczeństwie – kierunek „bezpieczeństwo narodowe”**. W tym zakresie Krakowska Szkoła Wyższa współpracuje z **Akademią Obrony Narodowej**.

Uczestników konferencji, w której wzięło udział kilkadziesiąt osób, w tym goście z partnerskich uczelni na Węgrzech i w Słowacji, przywitał przewodniczący komitetu organizacyjnego **prof. dr hab. Mirosław Kwieciński**, a otwarcia dokonał **kanclerz Krakowskiej Szkoły Wyższej prof. Klemens Budzowski** – jeden z czterech założycieli uczelni. W programie przewidziano 25 referatów, które zostały podzielone na siedem następujących sesji tematycznych:

- sesja I: „Bezpieczeństwo – nowa perspektywa inspiracji i badań naukowych”,
- sesja II: „Bezpieczeństwo – mit czy hit? Współczesna eskalacja zagrożeń oraz determinanty sukcesów w zachowaniu bezpieczeństwa” (panel ekspertów),
- sesja III: „Strategie bezpieczeństwa”,
- sesja IV: „Terror i terroryzm”,
- sesja V: „Bezpieczeństwo informacji”,
- sesja VI: „Edukacja na rzecz bezpieczeństwa”,
- sesja VII: „Bezpieczeństwo biznesu, gospodarki i społeczeństwa”.

Wspólnym mianownikiem zdecydowanej większości sesji było pojęcie bezpieczeństwa. Jak na konferencję naukową przystało, formułowano różne definicje tego pojęcia – jako nauki, jako wartości egzystencjalnej, wiążącej się m.in. z poczuciem stabilności i odczuciem braku stanu zagrożenia, jako jednego z „produktów, na którym można zarobić” (podejście ekonomiczne) i inne. Podczas panelu ekspertów zwrócono uwagę m.in. na różnicę pomiędzy zapewnianiem bezpieczeństwa (co nie jest w praktyce możliwe), a zapewnianiem poczucia bezpieczeństwa (co uzyskać jest dużo łatwiej).

Pojawiły się też cytaty wypowiedzi wybitnego myśliciela – Arystotelesa, a także twórcy psychoanalizy – Freuda. Poniższym cytatem z prof. Zygmunta Freuda, nawiązującym do pojęcia bezpieczeństwa, kończę relację z omawianej konferencji: *„Człowiek współczesny ma niezmierne trudności w trwałej, stałej i uzasadnionej realizacji swoich potrzeb, pragnień i zamiarów. Stąd przewartościowania dobra najwyższego ze szczęścia na bezpieczeństwo lub traktowanie bezpieczeństwa jako współczesnego, bardziej realnego substytutu szczęścia”.*

Adam Bułaciński, Redakcja

Skuteczna **detekcja**

wszechstronne zastosowania

IVORY - precyzyjna optyka zwierciadlana
AQUA Luna - nowatorskie rozwiązanie podświetlenia awaryjnego
AMBER - atrakcyjna, kompaktowa obudowa

Idealne rozwiązania do ochrony banków,
obiektów przemysłowych, biur,
jak również domów i mieszkań.

Satel®

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

TALOS - MOBILNY, AUTONOMICZNY SYSTEM NADZORU DO OCHRONY GRANIC LĄDOWYCH UE

TALOS (*Transportable, Adaptable Patrol for Land Border Surveillance System* - Transportowalny, Adaptowalny System Patrolowania i Nadzoru Granicy Lądowej) to międzynarodowy projekt badawczy, współfinansowany ze środków 7. Programu Ramowego Badań i Rozwoju Technologicznego Unii Europejskiej w obszarze "Inteligentny nadzór i bezpieczeństwo granic". Budżet projektu wyniesie 20 mln euro, z czego aż 13 mln euro będzie pochodzić od Komisji Europejskiej. Jest to obecnie największy w Polsce i jeden z najważniejszych w Europie projektów z dziedziny bezpieczeństwa

Konsorcjum projektowe skupia 14 organizacji z obszaru przemysłu, sfery badawczo-rozwojowej oraz szkolnictwa wyższego z ośmiu krajów członkowskich Unii oraz Turcji i Izraela.

Polskę reprezentuje czterech partnerów z Przemysłowym Instytutem Automatyki i Pomiarów (PIAP) na czele, w roli koordynatora. Projekt rozpoczął się w czerwcu bieżącego roku, a jego realizacja potrwa cztery lata.

System opracowany w ramach przedsięwzięcia oparty będzie na rozwiązaniach robotycznych. Jego celem jest pomoc w wykrywaniu, śledzeniu i przechwytywaniu osób usiłujących bezprawnie przekroczyć granicę.

TALOS obejmie trzy podstawowe elementy: bezzałogowe pojazdy naziemne i powietrzne, których zadaniem będzie patrolowanie granicy; naziemne wieże obserwacyjne, umieszczone na platformach mobilnych, oraz centrum dowodzenia zapewniające łączność pomiędzy elementami znajdującymi się w terenie a właściwą jednostką Straży Granicznej (rys. 1).

Tradycyjne systemy ochrony granic lądowych zbudowane są głównie z kosztownych obiektów naziemnych, rozmieszczonych wzdłuż całej granicy, które są używane do obserwacji, wykrywania i ostrzegania. Infrastruktura ta jest uzupełniana przez piesze i zmotoryzowane patrole strażników. Dzięki swojej mobilności system TALOS umożliwi zmniejszenie zapotrzebowania na stałe (nieruchome) elementy obserwacyjne i zabezpieczające (w tym ogrodzenia), a autonomiczność bezzałogowych jednostek, wyposażonych w dokładne modele terenu, skanery laserowe i systemy nawigacji najwyższej klasy, zniweluje potrzebę zaangażowania dużych zasobów ludzkich.

Wszystkie komponenty będą łatwe do transportowania – ich umieszczenie w standardowych kontenerach umożliwi szybkie przenoszenie systemu drogą powietrzną, lądową, morską i kolejową, a to oznacza możliwość błyskawicznego rozmieszczenia na dowolnie wybranym odcinku granicy.

Niezwykle ważną cechą systemu TALOS będzie jego duża skalowalność i zdolność adaptacji – jego architektura pozwoli na szybkie dostosowywanie go do warunków topograficznych i nasilenia nielegalnych działań na kontrolowanym terenie. Dobór rodzaju, liczby i wyposażenia bezzałogowych jednostek umożliwi dostosowanie systemu do długości odcinka granicy i charakteru nielegalnej działalności, a także łatwe przystosowanie go do działania w różnych warunkach terenowych.

TALOS umożliwi funkcjonariuszom Straży Granicznej reagowanie na nielegalne przekroczenie granicy w ciągu kilku minut. Bezzałogowy pojazd naziemny może zatrzymać intruza lub podążać za nim do momentu przybycia strażników. Dzięki temu podejrzany osobnik będzie pozostawał pod ciągłą obserwacją od momentu wykrycia go przez czujniki.

Rys. 1. Koncepcja działania systemu TALOS

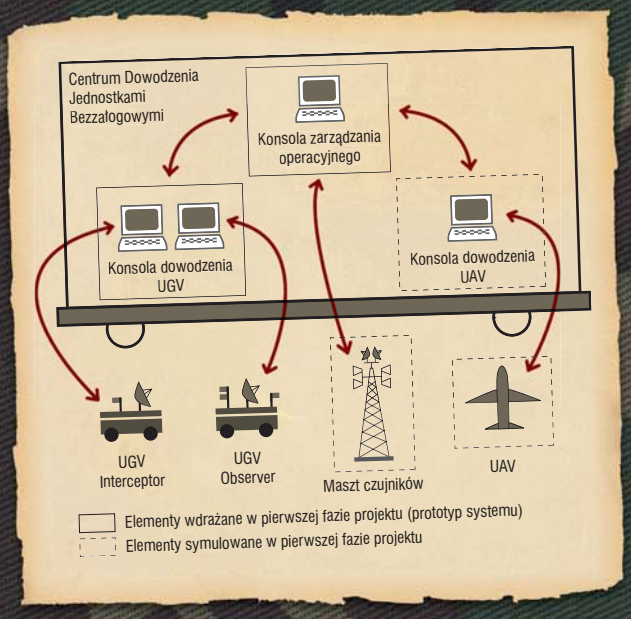
Prototyp systemu TALOS będzie się składać z Centrum Dowodzenia Jednostkami Bezzałogowymi (*Unmanned Units Command Centre* – UUCC) i dwóch Bezzałogowych Pojazdów Naziemnych (*Unmanned Ground Vehicles* – UGV). Bezzałogowy Samolot (*Unmanned Air Vehicle* – UAV) i mobilny Maszt Czujników (*Sensor Tower*) zostaną zintegrowane z systemem w przyszłości (rys. 2).

Kontrola nad operacją patrolujących pojazdów odbywać się będzie dzięki Centrum Dowodzenia Jednostkami Bezzałogowymi (UUCC). Specjalne konsole (*Operator Control Units* – OCU) posłużą dowódcy i operatorom jednostek przebywającym w Centrum do zarządzania misją i pojazdami. Na ekranie dowódcy misji prezentowana będzie wizualizacja obszaru działań z naniesionymi pozycjami elementów systemu, trasami patroli i danymi ze wszystkich sensorów. Operatorzy pojazdów otrzymają pełną kontrolę nad swoimi jednostkami, włącznie z możliwością sterowania ręcznego, planowania patrolu i przeglądania informacji z czujników.

Bezzałogowe Pojazdy Naziemne (UGV – fot. 1) będą stale patrolować wybrany odcinek granicy. Prototyp systemu TALOS zostanie wyposażony w ich dwie konfiguracje – **Observer** będzie stale patrolował granicę, a **Interceptor** posłuży do zatrzymania lub śledzenia ewentualnego intruza do czasu przybycia funkcjonariuszy Straży Granicznej. Drugi z pojazdów umożliwi też operatorowi komunikację z wykrytym osobnikiem, na przykład za pomocą mikrofonu i głośnika.

Bezzałogowy Samolot (UAV) zapewni nadzór z powietrza i znajdzie zastosowanie jako węzeł sieci komunikacyjnej. Przeznaczeniem mobilnych Masztów Czujników będą miejsca wymagające ciągłej obserwacji lub niedostępne dla pojazdów. UAV oraz Maszty Czujników nie wejdą w skład prototypu zrealizowanego w pierwszej fazie projektu. Żeby przygotować system TALOS do przyszłej integracji tych elementów, komunikacja z ich podsystemami będzie symulowana przez komputery w Centrum Dowodzenia.

Za dwa i pół roku demonstracyjna wersja systemu zostanie zaprezentowana Polskiej Straży Granicznej. Konsorcjum będzie kontynuować prace nad jego pełnym wdrożeniem na europejskich granicach zewnętrznych.



Rys. 2. Proponowana architektura systemu TALOS

Istotnym elementem realizacji projektu TALOS jest powołanie Komitetu Doradczego Użytkowników Końcowych składającego się z przedstawicieli straży granicznych państw członkowskich i kandydujących Unii Europejskiej, posiadających odcinki lądowej granicy Unii (Estonii, Grecji, Polski, Rumunii oraz Turcji). Zadaniem Komitetu będzie opiniowanie i nadzór nad prawidłowym zaprojektowaniem i wykonaniem systemu.

– *TALOS jest programem pionierskim w skali światowej, bowiem nikt jeszcze nie wykorzystywał robotów w tak szerokim zakresie w równie zróżnicowanym terenie. Jego wybór przez Komisję Europejską jest bezprecedensowym sukcesem, wynikającym zarówno z wieloletniego doświadczenia PIAP-u w realizacji zautomatyzowanych systemów wspierania działań służb mundurowych, jak i z ogromnych kompetencji i potencjału naszych partnerów. Ze względu na liczbę uczestników projektu jest to również znaczące wyzwanie organizacyjne. Chcemy rozwijać autonomiczne systemy robotyczne, ponieważ wierzymy, że staną się one w niedalekiej przyszłości ważnym elementem europejskiego systemu ochrony granic. Jesteśmy przekonani, że przyszłość konfrontacji z niebezpieczeństwem to roboty* – powiedział dr Jan Jabłkowski, dyrektor PIAP-u.

Mariusz Andrzejczak,
Agnieszka Sprońska

Ośrodek Systemów Bezpieczeństwa
Przemysłowy Instytut Automatyki i Pomiarów (PIAP)

Fot. 1. Bezzałogowy Pojazd Naziemny

Bezpieczeństwo aplikacji biznesowych

część 1

Bezpieczeństwo sieci

Firmy są dziś coraz bardziej zdane na informatykę i systemy informatyczne. Aplikacje kontrolują finanse, logistykę, wspomagają produkcję, jak również zarządzają skomplikowana aparaturą. Informatyka jest obecna na każdym kroku, jednak z jej używaniem wiąże się również bardzo dużo zagrożeń, o których czasami staramy się zapomnieć, mając na uwadze naglące terminy. Naciski zarządu i inne podobne sytuacje sprawiają, że szybko wdrażane systemy nie są w pełni szczelne. Dlatego, choć realia są czasami trudne, należy zawsze zwracać uwagę na aspekty związane z bezpieczeństwem systemów informatycznych. Czasem przeoczenie tylko jednego punktu bądź aspektu związanego z bezpieczeństwem może być opłakane w skutkach. Każda nowa technologia niesie również za sobą nowe luki bądź błędy i bieżące śledzenie informacji z odpowiednich źródeł (tych złych, jak strony hakerskie, jak również tych dobrych, jak na przykład CERT)

Artykuł ten ma na celu przedstawienie aspektów związanych z bezpieczeństwem aplikacji w następujących obszarach:

- bezpieczeństwo sieci, w tym bramy aplikacyjne i zapory sieciowe, systemy wykrywania intruzów i metody kryptograficzne;
- bezpieczeństwo infrastruktury, które dotyczy wysokiej dostępności, jak również wykonywania kopii bezpieczeństwa;
- bezpieczeństwo systemu operacyjnego i bazy danych, na której działają aplikacje;
- wewnętrzne mechanizmy zabezpieczające, osadzone już w samych aplikacjach.

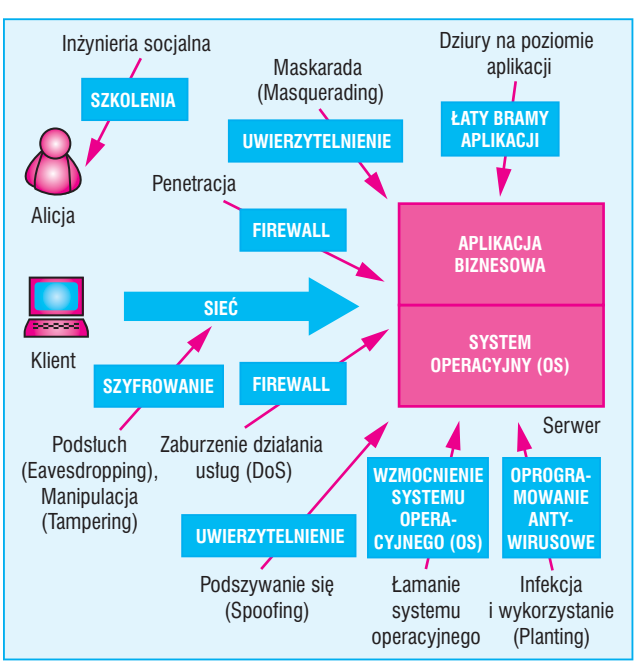
Część pierwsza artykułu będzie dotyczyć bezpieczeństwa sieci.

Architektura obecnych aplikacji biznesowych składa się obecnie z warstwy prezentacyjnej (dedykowany klient bądź przeglądarka internetowa) i serwera aplikacyjnego, który jest podłączony do bazy danych. Całość uruchamiana jest na danym systemie operacyjnym i współdzieli swoje usługi poprzez sieć lokalną bądź rozległą. Obecnie wiele takich aplikacji jest również udostępnianych w Internecie. W tym ostatnim przypadku należy zwrócić szczególną uwagę, gdyż do takich systemów dostęp ma teoretycznie każdy.

W dzisiejszych czasach również biznes chciałby mieć kontrolę nad tym, co dzieje się w aplikacjach, a nie tylko działy IT, które ukrywały to dotychczas jako wiedzę „tajemną". Jednak umożliwienie tego osobom, które nie są zaznajomione z technologiami informatycznymi, wiąże się także z dodatkowym ryzykiem. Z tego powodu zaczynają obecnie powstawać specjalne aplikacje, które, chroniąc zasoby IT, umożliwiają elastyczne zarządzanie nimi przez stronę biznesową. Dlatego też procesy związane z bezpieczeństwem zaczynają być coraz bardziej automatyzowane.

Bezpieczeństwo sieci

Pierwszym zagadnieniem związanym z bezpieczeństwem aplikacji biznesowych jest otoczenie sieciowe, w którym pracują. Bez sieci takie aplikacje byłyby bezużyteczne, gdyż nie mogłyby trafić do użytkownika. Obecnie duża większość sieci oparta jest na protokole TCP/IP (tym samym, na którym pracuje sieć Internet). Dlatego też wszystkie zagrożenia, jak również mechanizmy przechwycenia danych stosowane w Internecie, atakujący może z powodzeniem użyć do ataków wewnątrz sieci firmowej. Jest to o tyle groźne, że większość



Rys. 1. Zabezpieczenia kontra luki

Jak wygląda praca włamywacza
1. Rozeznanie
– zebranie informacji o infrastrukturze i konfiguracji, – zebranie informacji o systemie i aplikacji, – przegląd list dyskusyjnych przeznaczonych dla administratorów i programistów, – przegląd danych WHOIS[1], – użycie wyszukiwarek do znalezienia „ukrytych" plików na docelowym serwerze.
2. Analiza danych
– identyfikacja serwera sieciowego i systemu operacyjnego, – wyszukanie kluczowych informacji (metadanych, np. o autorze), – wyszukanie komentarzy w kodzie HTML, – wyszukanie kodu źródłowego wykonywalnego po stronie serwera, – przegląd wszystkich punktów kontaktowych aplikacji, – dedukcja całościowego bezpieczeństwa przez przegląd błędów, – analiza logiki aplikacji.
3. Przygotowanie ataku
– wykrycie, jak aplikacja może zareagować na nieprzewidziane wpisy, – próba oszukania logiki aplikacji, – stworzenie „wzorca" ataku.
4. Atak
– pobranie informacji/rezultatów, – wykonanie odpowiednich czynności (np. podmiany stron).
5. Czyszczenie
– kasowanie wpisów w logach, – kasowanie innych danych, umożliwiających śledzenie, – jeżeli to możliwe – instalacja backdoora[2].

1) WHOIS (ang. *who is* = kim jest) – protokół TCP oparty na zasadzie: pytanie/odpowiedź, który jest szeroko rozpowszechniony do wysyłania zapytań w celu poznania właściciela domeny, adresu IP lub innych informacji teleadresowych (źródło: Wikipedia – przyp. red.).
2) *Backdoor* (tylne drzwi) – luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania (źródło: Wikipedia – przyp. red.).

Tab. 1. Jak wygląda praca włamywacza

naruszeń bezpieczeństwa występuje z wnętrza firmy. Dlatego ochrona sieci jest jednym z istotnych zagadnień bezpieczeństwa całej infrastruktury.

Typowe zagrożenia sieciowe i stosowane przeciwko nim zabezpieczenia przedstawiono na rys. 1.

W bezpieczeństwie sieciowym można rozgraniczyć następujące obszary:

– **separację sieci** poprzez odpowiednie firewalle, czyli zapory ogniowe, które filtrują ruch z i do sieci;
– **systemy IDS** (*Intrusion Detection Systems*), czyli systemy, które monitorują cały ruch i wykrywają próby włamania bądź próby zaburzenia działania usług (tzw. DoS – *Denial of Service*);
– **kryptografię**, czyli wykorzystanie kryptologii do zapewnienia integralności danych, poufności w kanałach transmisyjnych, niezaprzeczalności, jak również umożliwienie stosowania podpisu cyfrowego;
– **czynnik ludzki**, czyli zapewnienie odpowiedniej edukacji pracownikom, w tym także szkoleń przeciwdziałających skutkom zastosowania tak zwanych technik socjalnych, czyli wyłudzania hasła, uzyskiwania nieuprawnionego, chociaż chronionego dostępu itd.

Zapora ogniowa (*firewall*)

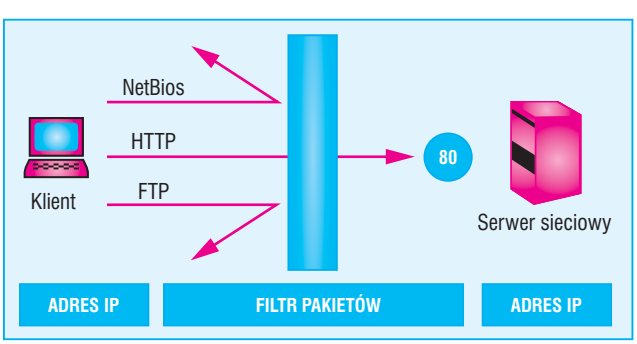
Pierwszym elementem, o który należy zadbać we właściwie zabezpieczonej sieci, jest zapora ogniowa, czyli *firewall*. Można ją stosować do łączenia różnych typów sieci, ich separacji czy tworzenia sieci zdemilitaryzowanych (takich, które łączą zasoby internetowe z zasobami intranetowymi). *Firewall* może być użyty jako filtr IP, filtrująca brama *Proxy* albo kombinacja obu tych mechanizmów.

Firewall jako filtr pakietów jest najprostszym mechanizmem i można go traktować jako bramę sieciową, sprawdzającą tylko nagłówek IP. Jest on efektywny kosztowo, bardzo szybki, łatwo konfigurowalny i całkowicie przeźroczysty dla aplikacji. Natomiast z drugiej strony narażony jest na ataki typu *IP spoofing* (podszywanie się). Trudne może być również utrzymanie reguł filtrowania.

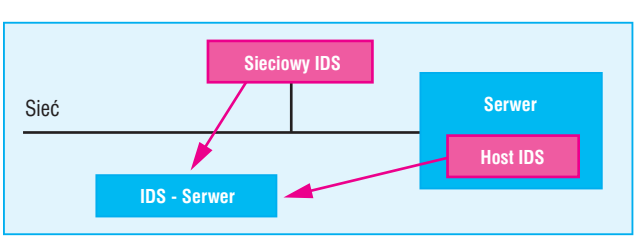
Następny typ *firewalla* to tak zwany *stateful packet filter*, czyli zaawansowany filtr pakietów (rys. 2).

Jest to typowe rozwiązanie *firewall*. Sprawdza adresy IP, jak również porty i sesje TCP, może także sprawdzać wzorce w przesyłanych danych. Może tworzyć dynamicznie reguły na podstawie wykrytego protokołu (np. DNS, NFS). Zapewnia bardzo dobry i ogólny poziom bezpieczeństwa. Z wad należy wymienić to, że może nie wykryć ataku na aplikację, może sam posiadać błędy, przez które atakujący może przełamać zabezpieczenia.

Najbardziej zaawansowanym typem *firewalla* jest brama aplikacyjna. Chroni ona już nie tylko poziom sieci, ale również to, co z sieci dociera do aplikacji. Często pakiety są przebudowywane w takiej bramie, a później trafiają do aplikacji. Zapora ogniowa oferuje bardzo wysoki poziom bezpieczeństwa, jednak nie jest przeźroczysta dla aplikacji, a jej konfiguracja jest często skomplikowana. *Firewall* może zawierać przy tym własne błędy. Jednak, działając jako pośrednik, jest w stanie autoryzować i przeprowadzać wstępną kontrolę tego, „co ktoś może i skąd", waliduje (zatwierdza) zapytania o usługę (np. sprawdza, czy w zapytaniu nie są użyte frazy, które powodują włamanie do aplikacji), zapewnia integralność i poprawność wiadomości (np. SOAP), możliwe jest także włączenie funkcji audytowych.



Rys. 2. Działanie filtru pakietów



Rys. 3. System wykrywania intruzów (IDS)

System wykrywania intruzów (IDS)

Systemy zapór ogniowych to jednak nie wszystko, dlatego następnym krokiem do zapewnienia bezpieczeństwa sieci jest zastosowanie systemu wykrywania intruzów (IDS), którego celem jest badanie ruchu sieciowego oraz monitorowanie i informowanie o niepożądanych akcjach (rys. 3).

System IDS składa się z jednego bądź wielu sieciowych i serwerowych sensorów, jak również z jednego bądź wielu systemów monitorowania i raportowania.

Sensor IDS instalowany na komputerze/serwerze

Sensor IDS instalowany na komputerze monitoruje lokalne zasoby systemu w zakresie zmian bądź nietypowych zachowań, obserwując logi systemowe, procesy systemowe i wykorzystanie zasobów. Uruchamiany w tle wysyła zawiadomienia do konsoli, na przykład wtedy, kiedy pojawiają się niepomyślne logowania.

Zalety:
- możliwość sprawdzania integralności systemu i danych,
- możliwość monitorowania szyfrowanej łączności,
- brak ograniczeń na topologię sieci (przełączalna sieć itp.),
- interpretacja danych w zależności od platformy.

Wady:
- możliwość tylko częściowego monitorowania stosu sieciowego,
- możliwość skompromitowania przez atak na sam system operacyjny bądź na IDS.

Sensory sieciowe IDS

Sensory sieciowe IDS monitorują cały ruch w sieci pomiędzy różnymi systemami, wyszukując specyficzne wzorce, identyfikując znane ataki albo poszukując niestandardowych zachowań. Są uruchamiane na specjalnym sprzęcie (*network sniffer*) albo integrowane z przełącznikami bądź ruterami – wysyłają komunikaty do konsoli na przykład w przypadku detekcji skanowania portów.

Zalety:
- są w stanie wykryć ataki na sieć,
- analizują „czyste" dane przepływające przez sieć,
- trudno jest je zaatakować bądź wykryć.

Wady:
- wymagają ciągłego zarządzania sygnaturami,
- generują dużo zgłoszeń podejrzeń o atak,
- nie ma możliwości analizowania szyfrowanego ruchu.

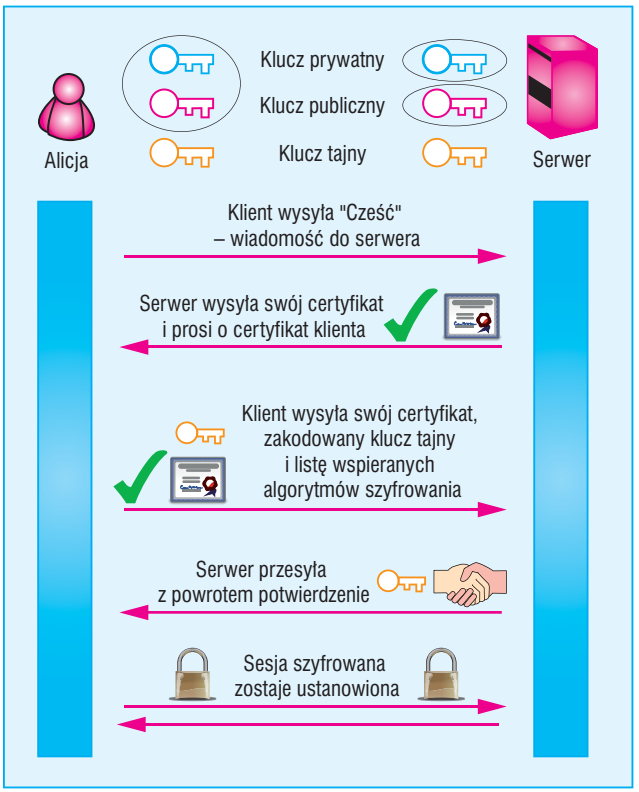
Powiązanie działania systemu IDS z *firewallem* może umożliwić blokadę ruchu atakującego, zanim przejmie on dane bądź wyrządzi szkody.

Kryptografia

Następną metodą zwiększającą bezpieczeństwo sieci jest stosowanie kryptografii. Kryptografia zapewnia bezpieczeństwo w paru obszarach, w zależności od sposobu jej użycia (tab. 2).

Obszar zapewniania bezpieczeństwa	Sposób użycia kryptografii
przeciwdziałanie podsłuchiwaniu	szyfrowanie
przeciwdziałanie podszywaniu się	autoryzacja
zapewnienie niezaprzeczalności	podpis cyfrowy

Tab. 2. Sposoby zapewniania bezpieczeństwa sieciowego przez kryptografię



Rys. 4. Etapy nawiązywania połączenia w SSL

Bezpieczeństwo oferowane przez kryptografię może również zostać wykorzystane do ataku – używając połączeń szyfrowanych (np. SSL), atakujący aplikację może ukryć się przed IDS bądź firewallem.

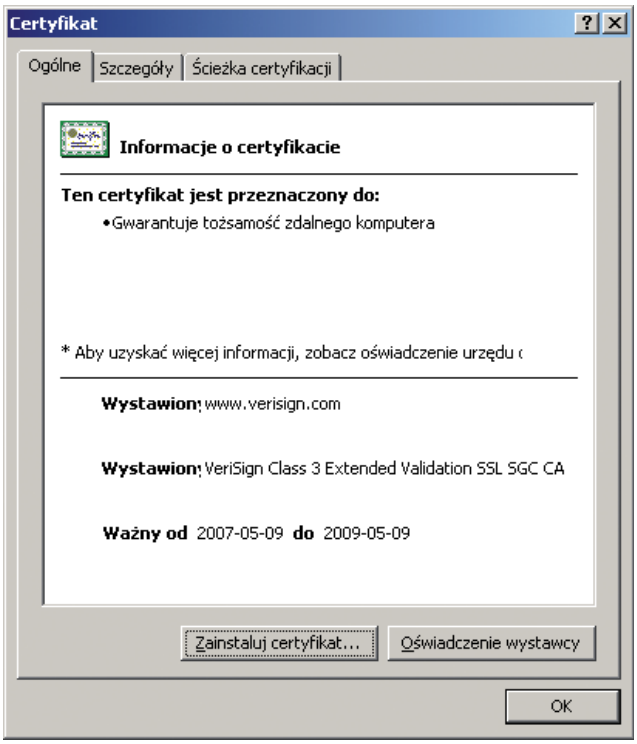
SSL (*Secure Socket Layer*) jest obecnie najbardziej popularnym protokołem, który służy do szyfrowania kanałów transmisyjnych (nagłówek protokołu i przeznaczenie poszczególnych jego części przedstawiono w tab. 3).

Nawiązanie połączenia w SSL ilustruje rys. 4.

Podczas uzgadniania połączenia klient i serwer negocjują, jakiej metody szyfrowania użyją, i wymieniają informację identyfikacyjną.

SSL Handshake Protocol	SSL Change Cipher Spec Protocol	SSL Alert Protocol	Application Protocols
– negocjacja algorytmu szyfrowania i jego parametrów – uwierzytelnienie serwera i opcjonalnie klienta – wymiana kluczy	– pojedynczy komunikat kończący połączenie SSL	– komunikaty o błędach (krytyczne błędy i ostrzeżenia)	
SSL Record Protocol			
– fragmentacja – kompresja – uwierzytelnienie wiadomości i ochrona integralności – szyfrowanie			
TCP			
IP			

Tab. 3. Nagłówek protokołu SSL



Rys. 5. Przykładowy certyfikat X.509

W komunikacji SSL używane są certyfikaty X.509, które mogą wyglądać tak, jak na rys. 5.

Certyfikaty X.509 są standardem internetowym dla bezpiecznych połączeń http. Umożliwiają autoryzację i szyfrowanie od strony serwera, jak również klienta. Używają dla ochrony metody symetrycznej, a także asymetrycznej.

Certyfikaty X.509 (zwane też certyfikatami elektronicznymi) mogą być użyte do pojedynczej autoryzacji, jak również w systemach jednokrotnego logowania (ang. *Single Sign-On* – SSO).

Każdy certyfikat zawiera:
- nazwę certyfikatu,
- nazwę centrum autoryzacyjnego (CA),
- okres ważności,
- klucz publiczny.

Zastosowanie szyfrowania przez SSL zwiększa jednak obciążenie systemów, gdyż SSL zwiększa standardowy czas odpowiedzi serwera o dwa dodatkowe cykle, wymagane w celu ustanowienia połączenia. Następuje także zwiększenie ilości przesyłanych danych o:
- SSL *handshake*,
- dodatkowy nagłówek używany przez SSL,
- zaszyfrowane dane.

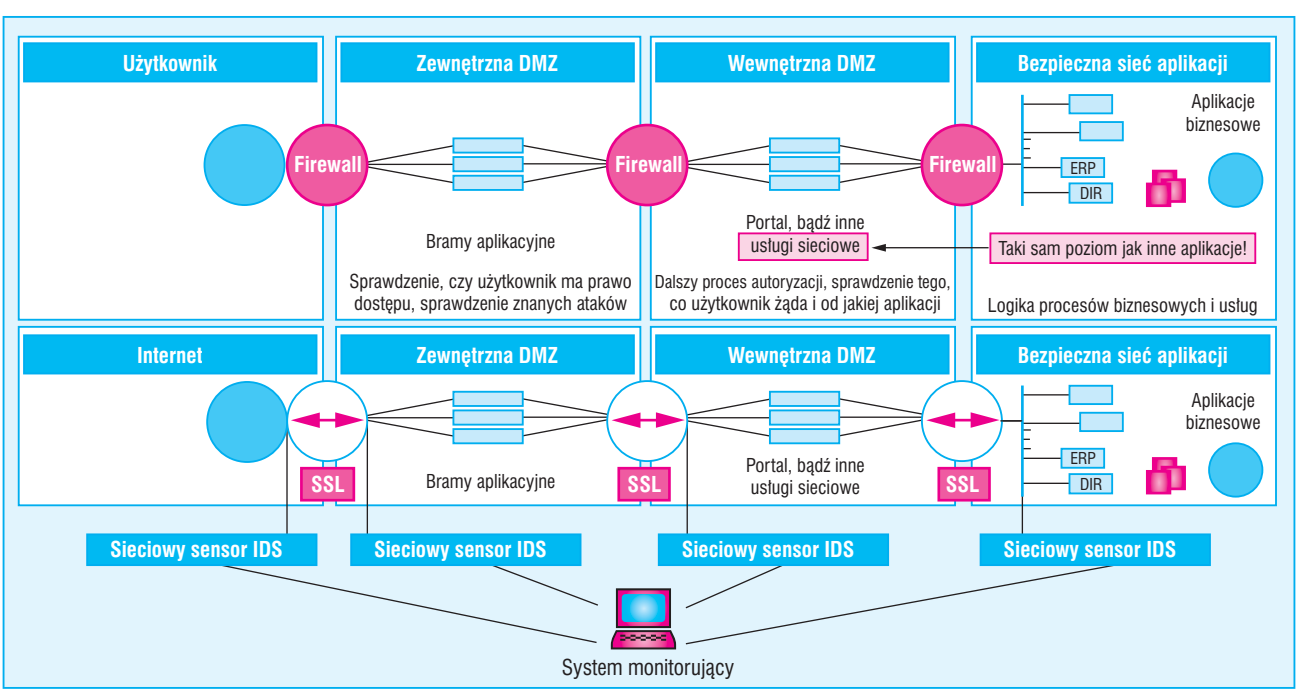
Obciążenie CPU może być o wiele większe i jest trudne do wstępnego oszacowania (z góry). Mocno zależy ono od scenariusza użycia – krótkie zapytania z różnych źródeł skutkują większym obciążeniem CPU niż określona liczba ustalonych połączeń SSL.

Podsumowując – bezpieczną architekturę sieciową można przedstawić tak, jak na rys. 6.

Aby zwiększyć bezpieczeństwo sieciowe, należy przestrzegać poniższych reguł:
- używać szyfrowanej komunikacji (np. SSL), kontrolować jakość haseł, reguł i czasu trwania sesji użytkownika, chronić użytkowników systemu operacyjnego, w którym pracuje aplikacja, jak również użytkowników bazy danych, ograniczyć uprawnienia technicznych użytkowników i administratorów do niezbędnego minimum,
- włączyć audyt i logowanie zdarzeń,
- uruchomić tylko niezbędne usługi i aplikacje,
- wgrywać regularnie poprawki i łaty, nie instalować wersji testowych ani demonstracyjnych na systemach produktywnych.

W drugiej części artykułu zostaną poruszone pozostałe zagadnienia związane z bezpieczeństwem aplikacji biznesowych, dotyczące infrastruktury oraz oprogramowania.

JACEK BUGAJSKI
SID GROUP



Rys. 6. Bezpieczna architektura sieciowa

artykuł sponsorowany

A to wszystko na jednej karcie…

W czasach tak rozwiniętej technologii plastikowa karta może mieć coraz szersze zastosowanie. Przykład stanowi karta kredytowa. Zastanówmy się, jakie daje możliwości:

- dostęp do strzeżonych obszarów,
- bezpieczne logowanie do komputera i sieci,
- płatność bezgotówkowa,
- rozliczanie w transporcie publicznym,
- pewność zamówień w programach lojalnościowych.

Pewną niedogodność stanowi fakt, iż każda z tych funkcji przypisana jest do innej karty, co zmusza użytkownika do posiadania coraz większej ich liczby. Zanim spróbujemy ułatwić użytkownikowi kart procedury, przyjrzyjmy się bliżej poszczególnym dostępnym technologiom:

- karty z paskiem magnetycznym – tradycyjne i efektywne kosztowo;
- karty zbliżeniowe 125 kHz – niezawodne i wygodne, ale z ograniczonym przeznaczeniem;
- inteligentne karty bezdotykowe – niezawodne i wygodne, elastyczne i bezpieczne;
- inteligentne karty dotykowe – skuteczne, elastyczne, bezpieczne, ale mniej wygodne;
- karty z kodem kreskowym – tanie i proste w obsłudze, lecz o nikim poziomie bezpieczeństwa.

Łączenie technologii

Powyższe cechy mogą zostać zamknięte w pojedynczej karcie. Praca na częstotliwościach 125 kHz i 13.56 MHz to połączenie technologii, które mogą ze sobą w łatwy sposób współdziałać. Pozostaje jedynie wybór jednej z dostępnych światowych technologii kart bezdotykowych spośród iCLASS, DESFire oraz Sony FeliCa. Tylko jeden z tych produktów może być umieszczony w pojedynczej karcie. Dodatkowo programowanie kart w formacie ISO daje możliwość nadrukowania na nich zdjęcia, co zwiększa przydatność w systemach kontroli dostępu.

Karty ISO są zbudowane w 100% z tworzywa PVC. Do pracy w ciężkich warunkach środowiskowych przeznaczone są karty zbudowane z tworzywa PVC oraz przezroczystego tworzywa PET (politereftalan etylenu).

Na rynku dostępne są również breloki do kluczy spełniające funkcje kart zbliżeniowych. Takie rozwiązanie sprawdza się doskonale w kontroli dostępu przy bramach wjazdowych na parking, furtach obrotowych czy zewnętrznych kontrolowanych przejściach. W przypadku wewnętrznej kontroli ciągłe noszenie przy sobie breloka z kluczami może stać się dla użytkownika uciążliwe.

Zastosowanie i bezpieczeństwo

Każda technologia cechuje się unikatowymi parametrami, odpowiadającymi określonym aplikacjom.

Karty z paskiem magnetycznym – efektywne pod względem ekonomicznym

Karty z paskiem magnetycznym są uniwersalne i efektywne pod względem ekonomicznym. W różnych obszarach aplikacji mogą przechowywać odpowiednio tekst, dane numeryczne i nieprzerobiony kod binarny. Dane są gromadzone w trzech różnych równoległych miejscach na pasku magnetycznym.

Na podstawie międzynarodowej umowy bankowej stworzono specjalny format kart magnetycznych ABA (*American Banking Association*), stanowiący standard kart kredytowych na całym świecie. Technologia ta jest również wykorzystywana przy systemach kontroli dostępu w obiektach edukacyjnych lub w podobnych środowiskach, w których wymagana jest duża przepustowość.

Cechą charakterystyczną kart magnetycznych jest ich trwałość, ale i stosunkowo niski poziom zabezpieczenia. W czytnikach kart magnetycznych zamontowana jest głowica podobna do głowic wykorzystywanych w odtwarzaczach kaset magnetofonowych. Przy każdym użyciu karty pasek magnetyczny zostaje przeciągnięty przez głowicę.

Równie łatwo można wykorzystać czytnik kart/koder do kopiowania kart. Tworzenie fałszywych kart kredytowych to przestępstwo dosyć rozpowszechnione na całym świecie.

Karty z kodem kreskowym – efektywne pod względem ekonomicznym

Karty z paskiem kodu kreskowego stanowią wizualny odpowiednik kart magnetycznych. Wzór równoległych linii tworzy kod binarny, który może reprezentować każdą informację alfanumeryczną. Karty z paskiem kodu kreskowego są zwykle używane w przemyśle, w celu finansowej kontroli pracy pracowników, oraz w handlu. Tego typu kart rzadko używa się w innych celach.

Karty zbliżeniowe 125 kHz – standard systemów kontroli dostępu

Początek technologii zbliżeniowej datuje się na 1972 rok, natomiast wzrost zainteresowania – na rok 1986. Koncepcja technologii zbliżeniowej wyklucza możliwość zepsucia zarówno karty, jak i czytnika. Z uwagi na to, że częstotliwość radiowa 125 kHz przesyłana jest przez każdy niemetaliczny materiał, można ukryć czytnik w ścianie przy montażu, a kartę nosić w portfelu lub torebce bez utraty sygnału.

Większość sprzedawanych czytników montowana jest wewnątrz chronionych obiektów, lecz sprawdzają się one również w zastosowaniach zewnętrznych, o ile nie są narażone na warunki arktyczne.

Między czytnikiem a kartą w technologii 125 kHz nie następuje kodowanie danych. Kody binarne są przechowywane na karcie i za każdym razem przesyłane do czytnika w tej samej postaci. Umożliwia to kopiowanie kart przy użyciu urządzeń o częstotliwościach radiowych. Mimo wielu podejrzeń i dyskusji na ten temat nie wykazano do tej pory przypadków nadużycia. Jednak dla zwiększenia bezpieczeństwa czytniki można wyposażyć w dodatkową klawiaturę lub czytnik biometryczny, które całkowicie ograniczają skuteczność kopiowania kart.

Inteligentne karty dotykowe – wysokie bezpieczeństwo logowania do komputera i sieci

Inteligentne karty dotykowe mają po jednej stronie metalizowane styki, umożliwiające komunikację z czytnikiem po umieszczeniu ich w nim. Karty te są wykorzystywane w logicznych systemach kontroli dostępu, pomiędzy kartą a komputerem lub innymi procesorami, ponieważ generują protokoły o wysokim standardzie bezpieczeństwa. Z uwagi na podatność czytników na warunki atmosferyczne i zagrożenie aktami wandalizmu rozwiązanie to nie jest wykorzystywane w systemach kontroli dostępu. Rozmiar pamięci do 256 kb oraz chip z kryptoprocesorem stanowią podstawę do wykorzystania w aplikacjach publicznych kluczy uwierzytelniających.

Inteligentne karty bezdotykowe – najbardziej elastyczne rozwiązanie w dziedzinie kart

Inteligentne karty bezdotykowe (iCLASS, DESFire itp.) działają na takich samych zasadach, jak karty zbliżeniowe z dodatkowym poziomem uwierzytelniania. Przy mniejszej pamięci niż karty kontaktowe oraz słabszym procesorze zapewniają porównywalny poziom integralności danych.

Proces obustronnego uwierzytelniania daje wynik 2^{80} zaszyfrowanych kombinacji pomiędzy czytnikiem i kartą. Kopiowanie karty staje się praktycznie niemożliwe. Pamięć na karcie jest podzielona. Skutkuje to tym, iż każda z aplikacji zabezpieczona jest unikatowym kluczem binarnym i tylko czytnik z odpowiednim kluczem jest w stanie odczytać dane.

Wszystko w jednym – rozwiązanie jednej karty w praktyce

Pracownik działu produkcji przychodzi do pracy i zatrzymuje się przy budynku produkcyjnym, gdzie swoją kartą 125 kHz otwiera bramę parkingową. Idzie do środka i za pomocą paska kodu kreskowego z karty uruchamia całą linię produkcyjną. Następnie pokazuje kartę z nadrukowanym zdjęciem strażnikowi, który przewozi go do budynku biurowego.

W nowym budynku biurowym wykorzystana została technologia 13.56 MHz i właśnie za pomocą takiej aplikacji w swojej karcie pracownik otwiera frontowe drzwi. Ta sama technologia umożliwia mu zakup napoju z automatu.

Aby dostać się do biura, pracownik musi przejść weryfikację biometryczną. Wzorzec siatkówki oka lub wzorzec odcisku palca zapisany w czytniku sprawdzany jest z tym, który jest zapisany w chipie karty.

W biurze pracownik wkłada swoją kartę do czytnika PC i udostępnia zaszyfrowane hasło do komputera. Po wprowadzeniu numeru PIN na klawiaturze czytnika zyskuje całościowy dostęp do wszystkich potrzebnych mu do pracy programów na komputerze i w sieci.

Podczas przerwy obiadowej korzysta z firmowej sali do ćwiczeń. Pasek z kodem kreskowym na jego karcie umożliwia mu włączenie światła w pomieszczeniu na 30 minut. Ponieważ zabrał kartę ze sobą na przerwę, jego komputer automatycznie wylogował go z wszystkich programów i pozostawił ekran w trybie czuwania. W ten sposób wszystkie dane na jego komputerze są bezpieczne.

Pod koniec dnia strażnik odwozi naszego przykładowego pracownika do jego samochodu. Aby pracownik mógł pojechać do domu, otwiera się, przy użyciu technologii 125 kHz, brama wyjściowa.

A to wszystko na jednej karcie…

Czesław Półtorak
HID Global

ZSJZ
AQAP 2110:2003

SYSTEM ZAPEWNIANIA JAKOŚCI PCBC
Certyfikowany na zgodność z PN-EN ISO 9001:2001

firma **ATLine®**

kompleksowe zabezpieczanie obiektów

15 LAT DOŚWIADCZENIA

BEZPIECZEŃSTWO W KAŻDYCH WARUNKACH

PROJEKTOWANIE... KOMPLEKSOWYCH DOKUMENTACJI

- TECHNICZNYCH, ARCHITEKTONICZNO - BUDOWLANYCH WRAZ Z NIEZBĘDNYMI BRANŻAMI SPECJALISTYCZNYMI OBIEKTÓW BIUROWYCH I PRZEMYSŁOWYCH
- INNOWACYJNYCH SYSTEMÓW OCHRONY
- TELETECHNICZNYCH, ELEKTRYCZNYCH I AUTOMATYKI PRZEMYSŁOWEJ

WYKONYWANIE...

ZAAWANSOWANYCH TECHNOLOGICZNIE SYSTEMÓW OCHRONY I BEZPIECZEŃSTWA

SPRZEDAŻ...

NOWOCZESNYCH SYSTEMÓW OCHRONY

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

GO MEGA

Przedstawiamy nową rodzinę megapikselowych kamer Sony

ZAPROJEKTOWANE Z MYŚLĄ O BEZPIECZEŃSTWIE

SONY

IPELA

Inteligentna analiza obrazu... bezpieczeństwo dla Ciebie

tel. +48 22 520 24 51, www.sonybiz.net/nvm

Blaski i cienie monitoringu IP
– przykład negatywny

Zanim przejdziemy do meritum sprawy, cofnijmy się w czasie o kilkadziesiąt lat i przypomnijmy sobie pierwsze centrale alarmowe Aplex z adresowalnymi liniami dozorowymi, jakie pojawiły się na polskim rynku w połowie lat osiemdziesiątych zeszłego stulecia. Były to znane większości instalatorów produkty firmy Europlex. Pamiętam jak dziś moduły adresowe LEM, podłączane do wspólnej magistrali, które rozmieszczało się na terenie obiektu w puszkach instalacyjnych lub nawet wkładało do wnętrza czujek, przez co okablowanie całego systemu znacznie się upraszczało. Nie miało to jeszcze nic wspólnego ze współczesnymi sieciami IP, w których poszczególne hosty też mają swoje adresy, ale był to jakby pierwszy krok w tym kierunku

Pamiętam także pewien szacowny obiekt, w którym była zainstalowana taka właśnie centrala, a ja miałem dokonywać okresowej konserwacji systemu alarmowego. Jakież było moje zdziwienie, gdy zajrzałem do szafy instalacyjnej i zobaczyłem wszystkie moduły LEM umieszczone w jednym miejscu, dosłownie obok siebie. Oczywiście w takiej sytuacji adresowalność systemu traciła jakikolwiek sens, zaś okablowanie czujek przybierało postać typowej gwiazdy. W miejsce nowoczesnej centrali z liniami adresowalnymi można było zastosować znacznie tańszy produkt o klasycznej konstrukcji, a efekt końcowy byłby prawdopodobnie lepszy, a już na pewno znacznie tańszy.

Minęło wiele lat, technologia systemów bezpieczeństwa zmieniła się diametralnie, lecz nawyki niektórych projektantów czy instalatorów jakby zatrzymały się w latach osiemdziesiątych zeszłego stulecia. W tym momencie należałoby wygłosić deklarację, typową dla filmów sensacyjnych, w stylu: „wszelkie podobieństwo do autentycznych osób, miejsc, wydarzeń jest przypadkowe...", ale niestety tak nie jest. Projekt, o którym chcę napisać, istniał naprawdę i inwestor zupełnie serio rozpatrywał możliwość jego realizacji.

O cyfrowych systemach monitoringu wizyjnego napisano już wiele i przeważnie pochlebnie. Zwolennicy tego typu instalacji wytaczają zazwyczaj te same argumenty, to znaczy:

- argument ekonomiczny – przy dużej liczbie kamer system IP jest tańszy od analogowego,
- argument techniczny – rozległy system IP jest łatwiejszy w obsłudze, konserwacji, odporniejszy na zakłócenia, łatwiejszy do rozbudowy niż system analogowy.

Czy jednak w codziennej praktyce projektowej sytuacja wygląda równie dobrze? Oczywiście, że nie, nie ma rzeczy idealnych, sieciowe systemy monitoringu wizyjnego też mają swoje wady i ograniczenia.

Chyba najistotniejszym z nich jest problem odległości. Większość kamer stosowanych w sieciowych systemach monitoringu wizyjnego do transmisji danych wykorzystuje interfejsy Fast Ethernet 100 Base TX, przystosowane do kabli miedzianych kategorii 5. Niestety już sam ten standard wprowadza ograniczenia, przewidując, że długości poszczególnych odcinków kabli łączących elementy aktywne nie mogą przekraczać 100 m (konkretnie 90 m + dwa giętkie odcinki końcowe po 5 m).

Jak więc sobie radzić w sytuacji, gdy kamery są rozlokowane w punktach odległych od serwerowni o kilkaset metrów? Zastosować punkty regeneracji danych? Jest to dobra i tania metoda, ale gdzie umieścić elementy aktywne, jak je chronić przed deszczem i z czego je zasilać? Przejść na łącza światłowodowe? To wymaga zupełnie innego okablowania oraz zmusza do stosowania kosztownych konwerterów. Zastosować łącza radiowe? Nie można, bo topografia terenu na to nie pozwala. Czy są jakieś inne wyjścia z tej sytuacji?

„Tak czy inaczej decyzja zapadła – to ma być system IP."

Owszem, na cytowanym przykładzie widać, że można sobie poradzić w jeszcze inny, aczkolwiek niekoniecznie prawidłowy sposób. Wyobraźmy sobie projekt sieciowego systemu monitoringu wizyjnego rozległych terenów otwartych bazujący na kamerach analogowych. Jak na razie nie ma w tym nic dziwnego, systemy hybrydowe są obecnie bardzo popularne, szczególnie w sytuacjach, gdy na terenie monitorowanych obiektów są już zainstalowane kamery, a chodzi jedynie o modernizację i unowocześnienie całej instalacji.

Jednakże w opisywanej sytuacji było inaczej. To miał być nowy system, budowany w obiekcie, który, jak to się mówi, „nie wyszedł jeszcze z ziemi". Projektant stanął na wysokości zadania i zaproponował nowoczesny system sieciowy. Możliwe, że taki był wymóg inwestora, a on się tylko dostosował. Tak czy inaczej decyzja zapadła – to ma być system IP.

Idąc dalej tym śladem, projektant chciał ograniczyć koszty inwestycji i przewidział zastosowanie tanich kamer analogowych i serwerów wizyjnych z interfejsami Fast Ethernet 100Base-TX, podłączonych do przełączników sieciowych kablami kategorii 5. Wspomniane przełączniki miały być połączone za pośrednictwem interfejsów 1000Base-T w sieć szkieletową, zaś jeden z nich, wyposażony w kilka interfejsów Ethernet 10GBase-T, miał posłużyć do podłączenia sieciowych rejestratorów wizyjnych. Całości instalacji miały dopełniać „odwrotne" serwery wizyjne, zamieniające ramki ethernetowe na sygnały analogowe do sterowania klasycznych monitorów z wejściami wizyjnymi. Co prawda z dokumentacji nie wynikało, jak te serwery mają być połączone z siecią, ale na użytek tej publikacji załóżmy, że było to zrobione prawidłowo.

„ ... projektant chciał ograniczyć koszty ... "

Z powyższego opisu nie wynikałoby nic nadzwyczajnego, gdyby nie fakt, że wszystkie wymienione powyżej urządzenia sieciowe zostały zlokalizowane w jednej szafie instalacyjnej! Innymi słowy połączenia sieciowe zamknęły się na powierzchni dwóch metrów kwadratowych, zaś transmisja sygnałów wizyjnych na rozległym terenie zewnętrznym odbywać się miała analogowo, za pośrednictwem kabli koncentrycznych. Czy taka instalacja w ogóle ma sens? Czy nie lepiej było zrezygnować z urządzeń sieciowych i zastosować zwykłe rejestratory analogowe?

Z ekonomicznego punktu widzenia wszystko to razem nie ma żadnego sensu, koszt pojedynczego serwera wizyjnego o odpowiedniej klasie i jakości przewyższa kilkukrotnie koszt dobrej kamery analogowej, więc nie ma mowy o zaoszczędzeniu na tanich kamerach. Przetwarzanie sygnału z postaci analogowej na cyfrową i odwrotnie, z cyfrowej na analogową, odbywać się miało dwa razy – raz przy kamerach i ponownie przy monitorach. Jedynym celem tych operacji było zapewnienie możliwości zastosowania rejestratorów cyfrowych, ale wobec przyjęcia obłędnej koncepcji całego systemu, polegającej na doprowadzeniu wszystkich sygnałów wizyjnych do serwerowni, lepiej byłoby zrezygnować z użycia serwerów wizyjnych, a te same pieniądze wydać na dobrej klasy rejestratory analogowe. Z całą pewnością efekt końcowy byłby lepszy.

Przyjrzyjmy się uważniej jeszcze jednemu istotnemu aspektowi proponowanej topologii systemu monitoringu. Jak projektant poradził sobie z problemem odległości? Sygnały analogowe ze wszystkich kamer miały być doprowadzone do serwerowni przy użyciu... kabli koncentrycznych, identycznych jak stosowane w osiedlowych instalacjach telewizji kablowej. Prawdopodobnie projektant liczył na ich małe tłumienie, nie przeszkadzała mu ich duża średnica ani sztywność, nie widział problemu w braku możliwości zainstalowania na ich końcach odpowiednich złącz.

„ ... połączenia sieciowe zamknęły się na powierzchni dwóch metrów kwadratowych"

Niewątpliwą i chyba jedyną zaletą proponowanego rozwiązania była bardzo niska cena tego typu kabla, która (jak sprawdziłem) wynosi 47 groszy za metr bieżący. Nie wiem, czy projektant w ogóle zastanawiał się nad tym, jak zachowa się kabel przeznaczony do transmisji sygnałów radiowych z zakresu fal decymetrowych podczas transmisji sygnału wizyjnego o widmie mieszczącym się w przedziale od prądu stałego do kilku MHz. Czy zastanowił się nad tym, że ten konkretny typ kabla ma żyłę środkową wykonaną z żelaza, o dużej rezystancji, co na długich trasach spowoduje bardzo silne stłumienie sygnału wizyjnego? Czy pomyślał o skuteczności ekranowania? Na koniec – czy wziął pod uwagę fakt, że ten konkretny typ kabla nie nadaje się do instalacji zewnętrznej? W jaki sposób chciał wprowadzić dziesiątki grubych, sztywnych kabli do pomieszczenia z aparaturą i jak chciał podłączyć je do rejestratorów umieszczonych w szafie instalacyjnej?

Jeśli pominąć absurdalność całej koncepcji i przyjąć, że ktoś chciałby koniecznie zrealizować tego typu pomysł, należałoby raczej zastosować typowy kabel RG59 w wersji ziemnej oraz kamery ze wzmacniaczami wyjściowymi, pozwalającymi na skorygowanie wpływu długości trasy kablowej. Chcąc uniknąć kryptoreklamy, wspomnę tylko, że typ tych kamer jest powszechnie znany na rynku telewizji dozorowej i że zapewniają one poprawną transmisję sygnałów wizyjnych na odległość do 1200 m. Możliwe, że nasz projektant tego nie wiedział, bo dotychczas zajmował się jedynie telewizją kablową i był to jego pierwszy projekt z dziedziny CCTV.

Jak widać, liczba popełnionych błędów jest tak duża, że nikt o zdrowych zmysłach w ogóle nie brałby tego projektu pod uwagę. Nikt poza inwestorem, który, nie będąc fachowcem w dziedzinie systemów monitoringu wizyjnego, zawierzył projektantowi i poparł chorą koncepcję systemu sieciowego, który de facto sieciowym nie był. Jak widać, nie wszystko złoto, co IP, zdrowy rozsądek nadal obowiązuje.

I tym stwierdzeniem kończę swój artykuł.

ANDRZEJ WALCZYK

Wprowadzenie do kosztorysowania systemów alarmowych (część 3)

Przykład kosztorysu systemu alarmowego

Niniejszy tekst stanowi kontynuację naszych wcześniejszych artykułów przybliżających zasady kosztorysowania robót branży zabezpieczenia technicznego. Przy nadmiarze informacji technicznej i technologicznej projektantom, instalatorom i inwestorom często umyka problematyka prowadzenia prawidłowej dokumentacji kosztorysowej i projektowej, wymaganej podczas realizacji inwestycji zabezpieczenia technicznego obiektu. Wynika to zarówno z technologicznej specyfiki wykonywania robót w branży zabezpieczenia technicznego, braku wzorców, niewiedzy projektantów i inwestorów, jak i ze skomplikowanych zagadnień formalnoprawnych. Dlatego pojawiła się idea przybliżenia tych zagadnień szerszemu kręgowi odbiorców na łamach pisma. Załączony kosztorys stanowi przykład opracowania kosztorysu inwestorskiego i został wykonany przy użyciu programu Norma PRO wersja 4.14a (licencja: 3136)

Projektowanie oraz kosztorysowanie stanowi nierozerwalny proces tworzenia kompleksowej dokumentacji zabezpieczenia obiektu.

Umiejętność wyceny kosztów wykonania systemu alarmowego stanowi część obowiązków projektanta systemów alarmowych.

Przypominamy, że zgodnie z aktualnym stanem prawnym szacowanie wartości inwestycji (kosztorysowania) ma miejsce:

- w przypadku finansowania całkowitego lub częściowego (dofinansowania) inwestycji ze środków publicznych (dofinansowanie), do których zalicza się także środki ze źródeł zagranicznych (od 1 maja 2004 r. środkami publicznymi są środki pochodzące z funduszy strukturalnych i spójności EU – art. 3 ustawy o finansach publicznych po zmianie);
- w przypadku ustalania wartości zamówienia publicznego na podstawie programu funkcjonalno-użytkowego, jeżeli przedmiotem zamówienia jest łącznie zaprojektowanie i wykonanie robót budowlanych.

Zanim przystąpimy do omawiania przykładowego kosztorysu, przypomnijmy także podstawowe etapy wykonywania systemu alarmowego.

Przebieg procesu inwestycyjnego systemu alarmowego należy rozpatrywać w następujących fazach:

1. Wykonanie instalacji przewodowej systemu oraz specjalnych połączeń pomiędzy urządzeniami wynikających z technologii lub wymagań producenta – okablowanie systemu, tj. klasyczne kable zasilające $230V_{AC}$ oraz w większości przypadków kable niskoprądowe $12V_{DC}$, koncentryczne itd., a obecnie zazwyczaj także kable ethernetowe, listwy itd.

2. Montaż urządzeń systemu (elementów – czujek, central, modułów sterujących, kart funkcyjnych itd.) – fizyczne mocowanie we wskazanych punktach wg projektu i wskazań producenta (zalecana wysokość, miejsce itd.).
3. Programowanie (oprogramowanie central alarmowych i modułów) – wykorzystanie możliwości konfiguracyjnych i programowych urządzeń do uzyskania parametrów wymaganych przez konkretny projekt i zapis właściwej konfiguracji w centrali alarmowej (urządzeniu sterującym, kontrolerze, serwerze itd.). Można tu wyróżnić:
   – programowanie urządzeń wg wymaganych parametrów pracy, funkcji i cech użytkowych (np. czułość czujki ruchu, parametry wykrywania ruchu przez sensor wizyjny itd.);
   – programowanie centrali alarmowej, głównego urządzenia sterującego, serwera itd. – przypisanie określonych cech użytkowo-funkcjonalnych i sposobów reakcji urządzeń centralowych na zagrożenia dzięki wykorzystaniu wbudowanego oprogramowania systemowego.
4. Programowanie zintegrowanego stanowiska bezpieczeństwa – wiąże się najczęściej z wydzielonym stanowiskiem PC (serwerem) i specjalnym programem, który pobiera informacje z centrali alarmowej, sterowników itd. i przedstawia je np. w formie graficznej.
5. Uruchomienie systemu (synchronizacja wszystkich elementów wg zadanego programu, zgodnie z dokumentacją techniczną).
6. Praca próbna systemu – testy działania wszystkich elementów systemu, sprawdzenie jego zaplanowanego wg projektu lub innych scenariuszy działania i reakcji na zagrożenia.
7. Szkolenie obsługi (różne poziomy: administratora, serwisanta, użytkownika).
8. Odbiór systemu alarmowego (kontrola systemu przed oddaniem go zamawiającemu do eksploatacji zgodnie z warunkami umownymi i dokumentacją).
9. Odbiór systemu – testy odbiorowe i potwierdzające założenia techniczno-funkcjonalne i użytkowe systemu zawarte w projekcie.
10. Konserwacja i serwis systemu alarmowego (niezbędne procedury i czynności utrzymania efektywnej sprawności działania systemu).
11. Bieżąca eksploatacja i modernizacja systemu alarmowego.
12. Uzupełniające szkolenia.

Zawartość i układ kosztorysu

Kosztorys posiada wymagany układ i zawartość, tj.:
– stronę tytułową, w której m.in. dokonano kwalifikacji robót wg Wspólnego Słownika Zamówień;
– ogólną charakterystykę obiektu, który zostanie zabezpieczony;
– książkę przedmiarów;
– kosztorys inwestorski;
– tabelę wartości elementów scalonych;
– kalkulację szczegółową cen jednostkowych pozycji.

Strona tytułowa

Opracowanie to jest jedną z ważniejszych części kosztorysu ze względów formalnych. Strona ta powinna zawierać następujące informacje:
– określenie rodzaju kosztorysu (ofertowy, inwestorski, zamienny lub powykonawczy) i ewentualnie jego numer w sytuacjach, gdy dla obiektu sporządza się wiele kosztorysów;
– nazwa obiektu i rodzaj robót objętych kosztorysem;
– lokalizacja i adres obiektu;
– firma i adres zamawiającego (inwestora);
– firma i adres wykonawcy robót (z wyłączeniem kosztorysu inwestorskiego);
– wartość kosztorysowa robót (w kosztorysie inwestorskim) lub cena kosztorysowa robót (w kosztorysach ofertowym, zamiennym i powykonawczym);
– nazwa i adres firmy sporządzającej kosztorys oraz nazwisko autora kosztorysu i jego podpis;
– zamieszczone na stronie tytułowej nazwiska i podpisy upełnomocnionych przedstawicieli oferenta (w kosztorysach ofertowych).

Poniżej przedstawiono przykład strony tytułowej kosztorysu inwestorskiego.

Strona tytułowa kosztorysu
xxxxxxxxxxxxxxx Warszawa, ul. Xxxxxxxxxxxx

Kosztorys Inwestorski
Klasyfikacja robót wg Wspólnego Słownika Zamówień

45312200-9 Instalowanie alarmów włamaniowych
45312100-8 Instalowanie pożarowych systemów alarmowych
45311100-1 Roboty w zakresie przewodów instalacji elektrycznej
45314200-3 Instalowanie infrastruktury kablowej

Nazwa inwestycji	Zabezpieczenie elektronicznymi systemami sygnalizacji zagrożeń
Adres inwestycji	Warszawa, ul. Xxxxxxxx
Inwestor	xxxxxxxxxxxxxxxxxxx
Adres inwestora	Warszawa, ul. Xxxxxxxx
Branża	Systemy zabezpieczeń technicznych
Sporządził kalkulację:	dr inż. Andrzej Wójcik
Data opracowania:	02.10.2007
Stawka roboczogodziny:	8.14 zł

Narzuty

Koszty pośrednie [Kp]	64.00% R, S
Koszty zakupu [Kz]	6.30% Mbezp
Zysk [Z]	11.80% R+Kp(R), S+Kp(S)
VAT [V]	22.00% Z(R+Kp(R)+Z(R), M+Kz(Mbezp), S+Kp(S)+Z(S))
Ogółem wartość kosztorysowa robót:	440 850.45 zł
Słownie:	**czterysta czterdzieści tysięcy osiemset pięćdziesiąt i 45/100 zł**

Wykonawca: Inwestor:

Data opracowania 02.10.2007 Data zatwierdzenia

Charakterystyka systemu alarmowego

Wymagane jest zaprezentowanie w sposób zwięzły charakterystyki wykonywanego w obiekcie systemu alarmowego. Charakterystyka powinna przedstawiać opis lokalizacji i topografię obiektu oraz zastosowane (planowane) systemy alarmowe z powołaniem się na odpowiednią normatywną ich klasyfikację, np. klasę zastosowanych systemów alarmowych, klasę urządzeń itd.

Ogólna charakterystyka systemu alarmowego realizowanego w obiekcie

Obiekt położony jest w kwadracie ulic: xxxxxxxxxxxxxxxxx na działce ewidencyjnej nr 00 w obrębie I-01-03 m. st. Warszawy w dzielnicy xxxxxx przy ul. xxxxxxxxx, zapisanej w jednostce rejestrowej 0000 nr 00000. Obiekt nie został wpisany przez wojewodę do ewidencji obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie. Właścicielem obiektu jest xxxxxxxxxxxxxxxxxx.

Obiekt graniczy od strony:
- północnej – z otwartym zagospodarowanym terenem z posadowionymi na nim szesnastopiętrowymi blokami mieszkalnymi;
- wschodniej – z ul. xxxxxxx, od której odgradza go ogrodzenie; w ogrodzeniu zamontowane są dwie bramy wjazdowe i cztery furtki wejściowe, po przeciwnej stronie ulicy znajduje się trzypiętrowy budynek mieszkalny i czteropiętrowy budynek, w którym mieści się zespół szkół średnich;
- południowej – z ul. xxxxxxxx, od której oddziela go ogrodzenie palisadowe wykonane z prętów metalowych; po przeciwnej stronie ulicy znajduje się kompleks bezpośrednio do siebie przylegających trzy-, czteropiętrowych budynków mieszkalnych;
- zachodniej – z parkingiem xxxxxxxxx, od którego oddziela go ogrodzenie palisadowe.

Na terenie obiektu znajduje się xxxxxxxxx wolnostojących budynków, których zasadnicze przeznaczenie jest następujące:
- biurowy X;
- biurowy Y;
- biurowy Z;
- budynek magazyn;
- budynek F;
- garaże;
- stacja trafo;
- budynek V.

Ochronie podlegają wskazane w dokumentacji projektowej pomieszczenia w budynkach xxxxx, teren wewnętrzny oraz wejścia i bramy xxxxxxx.

Obiekt został (zostanie) zabezpieczony systemami alarmowymi:
- sygnalizacji włamania i napadu;
- kontroli dostępu;
- telewizji dozorowej;
- sygnalizacji pożaru.

Systemy alarmowe zostały (zostaną) zintegrowane i są (będą) zarządzane przez zintegrowany system zarządzania bezpieczeństwem technicznym obiektu.

Ze względu na zaliczenie chronionego obiektu do III kategorii zagrożenia wartości zgodnie z PN-E-08390/14:1993 zastosowane systemy alarmowe posiadają klasę SA3, natomiast wybrane strefy ochrony będą posiadać systemy klasy SA4. Adekwatnie do klasy systemów alarmowych zastosowano urządzenia klasy C oraz w wybranych strefach ochrony urządzenia klasy S.

Zastosowane centrale alarmowe systemu sygnalizacji włamania posiadają 3 klasę zabezpieczenia.

Zastosowany system kontroli dostępu posiada 2 klasę rozpoznania i 3 klasę rozpoznania w wydzielonych strefach kontroli dostępu.

Oprócz tego podaje się krótki opis techniczny obiektu oraz charakterystykę jego elementów z uwzględnieniem w szczególności tych informacji, które mogą mieć wpływ na kalkulację ceny kosztorysowej (np. warunki gruntowe, rodzaj stolarki okiennej, ogrzewania budynku, zainstalowanego pieca, osprzętu elektrycznego itp.).

Poniżej znajduje się przykład takiej charakterystyki. Oczywiście opis będzie przygotowany pod kątem specyficznego obiektu, ale także z uwzględnieniem potrzeb zamawiającego.

Książka przedmiarów

Ustalanie ilości robót jest bardzo ważną czynnością poprzedzającą każdą kalkulację kosztorysową, sporządzaną zarówno metodą uproszczoną, jak i szczegółową. Dotyczy to zarówno kosztorysów sporządzanych przez inwestorów, jak też kosztorysów przygotowywanych przez wykonawców robót.

Od dokładności i poprawności określenia ilości robót zależy ostateczne oszacowanie kosztów lub ustalenie ceny kosztorysowej poszczególnych robót, elementów robót i całego obiektu, dla którego kalkulacja jest prowadzona.

Można stwierdzić, że nie ma kosztorysowania bez przedmiarowania.

Zakres robót ustala się na podstawie dokumentacji projektowej (przed przystąpieniem do realizacji robót) bądź sporządzonej na placu budowy dokumentacji budowy (po wykonaniu robót).

Dokument, w którym określa się ilość robót, nazywamy przedmiarem lub obmiarem robót.

Opracowanie przedmiaru robót jest pomocne na etapie:

1. Postępowania o udzielenie zamówienia

Celem przedmiaru robót jest dostarczenie wykonawcom, którzy biorą udział w postępowaniu o udzielenie zamówienia, informacji umożliwiających sprawne wyliczenie cen szczegółowych, odniesionych do poszczególnych pozycji przedmiaru, i opracowanie kosztorysów (zwanych także „wycenionymi przedmiarami robót") będących załącznikami do oferty w trybie przetargowym lub podstawą uzgodnień i wyboru wykonawcy w trybie negocjacji czy zamówienia z wolnej ręki.

2. Realizacji umowy

Celem przedmiaru robót jest umożliwienie ustalania wartości wykonanych robót na potrzeby bieżących rozliczeń wybranego wykonawcy z zamawiającym.

Pojęcie przedmiaru robót zostało zdefiniowane w wymienionych poniżej przepisach i opracowaniach. I tak w rozporządzeniu Ministra Infrastruktury z dnia 2 września 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz. U. Nr 202 z 16 września 2004 r., poz. 2072) w § 6 ust. 1 podano następującą definicję:

> *„Przedmiar robót jest to opracowanie zawierające zestawienie przewidywanych do wykonania robót podstawowych w kolejności technologicznej ich wykonania wraz z ich szczegółowym opisem lub wskazaniem podstaw ustalających szczegółowy opis oraz wskazaniem właściwych specyfikacji technicznych wykonania i odbioru robót budowlanych, z wyliczeniem i zestawieniem ilości jednostek przedmiarowych robót podstawowych".*

Oczywiście istnieją inne zbieżne definicje wynikające z praktyki środowiskowej, np. „Środowiskowe Metody Kosztorysowania Robót Budowlanych", które zostały wydane przez Stowarzyszenie Kosztorysantów Budowlanych oraz Zrzeszenie Biur Kosztorysowania Budowlanego, czy też norma PN-ISO 67047-2 (z 2000 roku): „Budownictwo. Terminologia. Terminy stosowane w umowach", która w punkcie 3.5.3. definiuje przedmiar robót w sposób następujący:

> *„Dokument przetargowy, przygotowany zazwyczaj w znormalizowanej formie, zawierający: opis robót w kolejności technologicznej ich wykonania, wykaz materiałów, ilość i sposób wykonania robót".*

Zgodnie z § 4 ust. 1 rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 r. (o którym mowa wyżej) przedmiar robót stanowi część składową dokumentacji projektowej, służącej do opisu przedmiotu zamówienia, co znaczy, iż za jego sporządzenie odpowiada projektant.

Obmiar robót (obliczenie ilości robót na podstawie pomiarów z natury) jest to opracowanie sporządzane po wykonaniu robót przez ich wykonawcę na podstawie książki obmiarów, niezbędne do wykonania kosztorysu powykonawczego lub zamiennego. Obmiar powinien zawierać opis poszczególnych wykonanych robót w kolejności technologicznej ich wykonania oraz podstawy do ustalenia cen jednostkowych robót lub jednostkowych nakładów rzeczowych (w kalkulacji szczegółowej) z podaniem ilości jednostek obmiarowych robót.

Obmiar robót ma za zadanie określać faktyczny zakres wykonanych robót wg stanu na dzień jego przeprowadzenia. Roboty można uznać za wykonane pod warunkiem, że wykonano je zgodnie z wymaganiami zawartymi w projekcie wykonawczym i szczegółowymi specyfikacjami technicznymi, a ich ilość podaje się w jednostkach ustalonych w wycenionym przedmiarze robót wchodzącym w skład umowy.

Obmiaru robót dokonuje wykonawca po pisemnym powiadomieniu zarządzającego realizacją umowy o zakresie i terminie obmiaru. Zaleca się, aby powiadomienie poprzedzało obmiar co najmniej o trzy dni. Wyniki obmiaru są wpisywane do księgi obmiaru i zatwierdzane przez inspektora nadzoru inwestorskiego.

W tabeli 1 przedstawione zostały wybrane fragmenty przedmiarów poszczególnych systemów alarmowych.

Przykład kosztorysu inwestorskiego

W tabeli 2 załączony został przykład kosztorysu ofertowego na realizację systemów alarmowych. Kosztorys należy budować wg etapów omówionych we wstępie artykułu, a dla przejrzystości oraz kontroli technologicznej trzeba podzielić pozycje kosztorysowania poszczególnych systemów na działy, tj. dział 1 – system kontroli dostępu, dział 2 – system telewizji dozorowej itd.

Wymienione etapy nie zawsze występują podczas realizacji przez jednego wykonawcę. Ze względu na technologię zastosowany system alarmowy może wręcz nie wymagać realizacji jakiegoś etapu. Przykładem na to jest realizacja bezprzewodowego systemu alarmowego, w której nie występuje etap instalacji przewodowej, lecz występuje etap instalacji transmisji bezprzewodowej.

NOVUS®

Czas na NOVUS®

Wybierz optymalne bezpieczeństwo

Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

Lp.	Podstawa	Opis i wyliczenia	j.m.	Poszcz.	Razem
Niniejszy kosztorys stanowi wycenę zabezpieczenia elektronicznymi systemami sygnalizacji zagrożeń w budynku xxxxxxx, tj. systemami: – **sygnalizacji włamania i napadu,** – **kontroli dostępu,** – **telewizji dozorowej,** – **sygnalizacji pożarowej,** – **integracji**					
1	**System sygnalizacji włamania i napadu**				
1 d.1	**KNR AL-01 0101-02**	Montaż kompaktowej centrali alarmowej do 8 linii dozorowych	szt.	1.000	
				RAZEM	**1.000**
		...			
30 d.1	**KNR AL-01 0601-01**	Przygotowanie i testowanie oprogramowania systemu alarmowego - do 25 kroków programowych (instrukcji)	n-g	1.000	
				RAZEM	**1.000**
2	**System kontroli dostępu**				
31 d.2	**KNR AL-01 0302-01**	Montaż elementów systemu kontroli dostępu - kontroler (sterownik) dla 1 wejścia kontrolowanego	szt.	23.000	
				RAZEM	**23.000**
		...			
43 d.2	**KNR AL-01 0307-04**	Praca próbna systemu kontroli dostępu - próby pomontażowe elektromagnetycznych elementów blokujących	szt.	19.000	
				RAZEM	**19.000**
44 d.2	**KNR AL-01 0306-03**	Uruchomienie systemu kontroli dostępu	szt.	19.000	
				RAZEM	**19.000**
3	**System sygnalizacji pożarowej**				
45 d.3	**KNR AL-01 0401-01**	Montaż czujek pożarowych - optyczna dymu	szt.	126.000	
				RAZEM	**126.000**
		...			
69 d.3	**KNR AL-01 0602-06**	Sprawdzenie i uruchomienie systemu	szt.	1.000	
				RAZEM	**1.000**
4	**System telewizji dozorowej**				
70 d.4	**KNR AL-01 0501-01**	Montaż elementów systemu telewizji dozorowej - kamera wewnętrzna	szt.	5.000	
				RAZEM	**5.000**
		...			
77 d.4	**KNR AL-010506-01**	Uruchomienie systemu telewizji dozorowej - linia transmisji wizji	linia	10.000	
				RAZEM	**10.000**
5	**System integracji**				
78 d.5	**KNR AL-01 0701-01 cena zakładowa**	Montaż standardowego zestawu PC, oprogramowania systemowego	szt.	1.000	
				RAZEM	**1.000**
79 d.5	**KNR AL-01 0702-04 analiza indywidualna**	Zainstalowanie oprogramowania zarządzającego systemami alarmowymi (od 15 do 20 MB)	kpl.	1.000	
				RAZEM	**1.000**
80 d.5	**KNR AL-01 0702-06 analiza indywidualna**	Programowanie i uruchomienie oprogramowania zarządzającego i nadzorującego systemy alarmowe	instr.	500.000	
				RAZEM	**500.000**
81 d.5	**KNR AL-01 0703-04 analiza indy widualna**	Dodatek za utrudnienia przy uruchamianiu oprogramowania systemowego i zarządzającego z tytułu trudności algorytmu - średniej trudności	wariant	500.000	
				RAZEM	**500.000**

Tab. 1. Książka przedmiarów (wybrane wpisy)

Lp.	Podstawa	Opis	Jedn. obm.	Ilość	Cena jedn.	Wartość
Niniejszy kosztorys stanowi wycenę zabezpieczenia elektronicznymi systemami sygnalizacji zagrożeń w budynku xxxxxxx, tj. systemami: – **sygnalizacji włamania i napadu,** – **kontroli dostępu,** – **telewizji dozorowej,** – **sygnalizacji pożaru,** – **integracji**						
1	**System sygnalizacji włamania i napadu**					
1 d.1	**KNR AL-01 0101-02**	Montaż kompaktowej centrali alarmowej do 8 linii dozorowych	szt.	1	938.77	938.77
		...				
30 d.1	**KNR AL-01 0601-01**	Przygotowanie i testowanie oprogramowania systemu alarmowego - do 25 kroków programowych (instrukcji)	n-g	1	5267.49	5267.49
					Razem dział:	**44327.95**
2	**System kontroli dostępu**					
31 d.2	**KNR AL-01 0302-01**	Montaż elementów systemu kontroli dostępu - kontroler (sterownik) dla 1 wejścia kontrolowanego	szt.	23	2374.02	54602.46
		...				
43 d.2	**KNR AL-01 0307-04**	Praca próbna systemu kontroli dostępu - próby pomontażowe elektromagnetycznych elementów blokujących	szt.	19	34.77	660.63
44 d.2	**KNR AL-01 0306-03**	Uruchomienie systemu kontroli dostępu	szt.	19	154.77	2940.63
					Razem dział:	**129304.45**
3	**System sygnalizacji pożarowej**					
45 d.3	**KNR AL-01 0401-01**	Montaż czujek pożarowych - optyczna dymu	szt.	126	267.22	33669.72
		...				
69 d.3	**KNR AL-01 0602-06**	Sprawdzenie i uruchomienie systemu	szt.	1	88.36	88.36
					Razem dział:	**117503.93**
4	**System telewizji dozorowej**					
70 d.4	**KNR AL-01 0501-01**	Montaż elementów systemu telewizji dozorowej - kamera wewnętrzna	szt.	5	851.67	4258.35
		...				
77 d.4	**KNR AL-01 0506-01**	Uruchomienie systemu telewizji dozorowej - linia transmisji wizji	linia	10	27.61	276.10
					Razem dział:	**54036.43**
5	**System integracji**					
78 d.5	**KNR AL-01 0701-01 cena zakładowa**	Montaż standardowego zestawu PC, oprogramowania systemowego	szt.	1	4711.28	4711.28
79 d.5	**KNR AL-01 0702-04 analiza indywidualna**	Zainstalowanie oprogramowania zarządzającego systemami alarmowymi o pojemności od 15 do 20 MB	kpl.	1	6293.79	6293.79
80 d.5	**KNR AL-01 0702-06 analiza indywidualna**	Programowanie i uruchomienie oprogramowania zarządzającego i nadzorującego systemy alarmowe	instr.	500	0.36	180.00
81 d.5	**KNR AL-01 0703-04 analiza indywidualna**	Dodatek za utrudnienia przy uruchamianiu oprogramowania systemowego i zarządzającego z tytułu trudności algorytmu - średniej trudności	wariant	500	9.99	4995.00
					Razem dział:	**16180.07**
					Wartość kosztorysowa robót bez podatku VAT	**361352.83**
					Podatek VAT	**79497.62**
					Ogółem wartość kosztorysowa robót	**440850.45**
					Słownie: czterysta czterdzieści tysięcy osiemset pięćdziesiąt i 45/100 zł	

Tab. 2. Kosztorys inwestorski (wybrane wpisy)

Poz.	Podstawa wyceny	Opis pozycji kosztorysowej	Jedn. miary	Nakłady na jedn.	Cena jednostkowa zł	Koszt jednostkowy zł
1	**System sygnalizacji włamania i napadu**					
1 d.1	**KNR AL-01 0101-02** 999	Montaż kompaktowej centrali alarmowej do 8 linii dozorowych	szt.			
		- Robocizna -	r-g	17.6000	8.14	143.264
		- Materiały - centrala alarmowa - procesor xxxxx	szt.	1.0000	636.02	636.020
		Koszty pośrednie od (R, S)	%	64.00	143.264	91.689
		Koszty zakupu od (Mbezp)	%	6.30	636.020	40.069
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	234.953	27.724
		Razem pozycja 1				**938.770**
		...				
30 d.1	**KNR AL-01 0601-01** 999	Przygotowanie i testowanie oprogramowania systemu alarmowego - do 25 kroków programowych (instrukcji)	n-g			
		- Robocizna -	r-g	17.6000	8.14	143.264
		- Materiały - oprogramowanie systemu KD	szt.	1.0000	4708.20	4708.200
		Koszty pośrednie od (R, S)	%	64.00	143.264	91.689
		Koszty zakupu od (Mbezp)	%	6.30	4708.200	296.617
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	234.953	27.724
		Razem pozycja 30				**5267.490**
2	**System kontroli dostępu**					
31 d.2	**KNR AL-01 0302-01** 999	Montaż elementów systemu kontroli dostępu - kontroler (sterownik) dla 1 wejścia kontrolowanego	szt.			
		- Robocizna -	r-g	7.8700	8.14	64.062
		- Materiały - kontroler (1 drzwi) xxxxxx	szt.	1.0000	2122.82	2122.820
		Koszty pośrednie od (R, S)	%	64.00	64.062	41.000
		Koszty zakupu od (Mbezp)	%	6.30	2122.820	133.738
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	105.062	12.397
		Razem pozycja 31				**2374.020**
		...				
41 d.2	**KNR AL-01 0601-01** 999	Przygotowanie i testowanie oprogramowania systemu alarmowego - do 25 kroków programowych (instrukcji)	n-g			
		- Robocizna -	r-g	17.6000	8.14	143.264
		- Materiały - oprogramowanie systemu kontroli dostępu	szt.	1.0000	4708.20	4708.200
		Koszty pośrednie od (R, S)	%	64.00	143.264	91.689
		Koszty zakupu od (Mbezp)	%	6.30	4708.200	296.617
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	234.953	27.724
		Razem pozycja 41				**5267.490**
		...				
43 d.2	**KNR AL-01 0307-04** 999	Praca próbna systemu kontroli dostępu - próby pomontażowe elektromagnetycznych elementów blokujących	szt.			
		- Robocizna -	r-g	2.3300	8.14	18.966
		Koszty pośrednie od (R, S)	%	64.00	18.966	12.138
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	31.104	3.670
		Razem pozycja 43				**34.474**
44 d.2	**KNR AL-01 0306-03** 999	Uruchomienie systemu kontroli dostępu	szt.			
		- Robocizna -	r-g	10.3700	8.14	84.412
		Koszty pośrednie od (R, S)	%	64.00	84.412	54.024
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	138.436	16.335
		Razem pozycja 44				**154.770**
3	**System sygnalizacji pożarowej**					
45 d.3	**KNR AL-01 0401-01** 999	Montaż czujek pożarowych - optyczna dymu	szt.			
		- Robocizna -	r-g	1.5500	8.14	12.617
		- Materiały - Czujka optyczna dymu SSD531/OSD2000	szt.	1.0000	229.62	229.620
		Koszty pośrednie od (R, S)	%	64.00	12.617	8.075
		Koszty zakupu od (Mbezp)	%	6.30	229.620	14.466
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	20.692	2.442
		Razem pozycja 45				**267.220**
		...				
69 d.3	**KNR AL-01 0602-06** 999	Sprawdzenie i uruchomienie systemu	szt.			
		- Robocizna -	r-g	5.9200	8.14	48.189
		Koszty pośrednie od (R, S)	%	64.00	48.189	30.841
		Zysk od (R+Kp(R), S+Kp(S))	%	11.80	79.030	9.326
		Razem pozycja 69				**88.360**

Tab. 3. Kalkulacja szczegółowa cen jednostkowych pozycji (wybrane wpisy)

4	**System telewizji dozorowej**					
70 d.4	**KNR AL-01 0501-01** 999	Montaż elementów systemu telewizji dozorowej - kamera wewnętrzna	szt.			
		- Robocizna -	r-g	3.3600	8.14	27.350
		- Materiały - kamera kolor, 520 TVL 0,3 lx AI/EI/BLC/AGC 12V DC/24V AC SCC-131 BP	szt.	1.0000	754.02	754.020
		Koszty pośrednie od (R, S) Koszty zakupu od (Mbezp) Zysk od (R+Kp(R), S+Kp(S)) **Razem pozycja 70**	% % %	64.00 6.30 11.80	27.350 754.020 44.854	17.504 47.503 5.293 **851.670**
		...				
75 d.4	**KNR AL-01 0506-01** 999	Uruchomienie systemu telewizji dozorowej - linia transmisji wizji	linia			
		- Robocizna -	r-g	1.8500	8.14	15.059
		Koszty pośrednie od (R, S) Zysk od (R+Kp(R), S+Kp(S)) **Razem pozycja 75**	% %	64.00 11.80	15.059 24.697	9.638 2.914 **27.610**
		...				
77 d.4	**KNR AL-01 0506-01** 999	Uruchomienie systemu telewizji dozorowej - linia transmisji wizji	linia			
		- Robocizna -	r-g	1.8500	8.14	15.059
		Koszty pośrednie od (R, S) Zysk od (R+Kp(R), S+Kp(S)) **Razem pozycja 77**	% %	64.00 11.80	15.059 24.697	9.638 2.914 **27.610**
5	**System integracji**					
78 d.5	**KNR AL-01 0701-01 cena zakładowa** 999	Montaż standardowego zestawu PC, oprogramowania systemowego	szt.			
		- Robocizna -	r-g	33.7000	8.14	274.318
		- Materiały - komputer xxxxxxx S2500/515MB/120GB/ 5200-128/DVDRW płyta główna xxxxxxx 8vt800, procesor xxxxxxx, HDD 120GB, klawiatura + mysz, monitor LCD 19" xxxxxxx, drukarka xxxxxxx, system operacyjny xxxxxxx	 szt. szt. szt. kpl.	 1.0000 1.0000 1.0000 1.0000	 1498.60 1256.70 377.60 826.00	 1498.600 1256.700 377.600 826.000
		Koszty pośrednie od (R, S) Koszty zakupu od (Mbezp) Zysk od (R+Kp(R), S+Kp(S)) **Razem pozycja 78**	% % %	64.00 6.30 11.80	274.318 3958.900 449.882	175.564 249.411 53.086 **4711.280**
79 d.5	**KNR AL-01 0702-04 analiza indywidualna** 999	Zainstalowanie oprogramowania zarządzającego systemami alarmowymi o pojemności od 15 do 20 MB	kpl.			
		- Robocizna -	r-g	1.4800	8.14	12.047
		- Materiały - Oprogramowanie Integracyjne wg technologii dostawcy	kpl.	1.0000	5900.00	5900.000
		Koszty pośrednie od (R, S) Koszty zakupu od (Mbezp) Zysk od (R+Kp(R), S+Kp(S)) **Razem pozycja 79**	% % %	64.00 6.30 11.80	12.047 5900.000 19.757	7.710 371.700 2.331 **6293.790**
80 d.5	**KNR AL-01 0702-06 analiza indywidualna** 999	Programowanie i uruchomienie oprogramowania zarządzającego i nadzorującego systemy alarmowe	instr.			
		- Robocizna -	r-g	0.0239	8.14	0.195
		Koszty pośrednie od (R, S) Zysk od (R+Kp(R), S+Kp(S)) **Razem pozycja 80**	% %	64.00 11.80	0.195 0.320	0.125 0.038 **0.360**
81 d.5	**KNR AL-01 0703-04 analiza indywidualna** 999	Dodatek za utrudnienia przy uruchamianiu oprogramowania systemowego i zarządzającego z tytułu trudności algorytmu - średniej trudności	wariant			
		- Robocizna -	r-g	0.6690	8.14	5.446
		Koszty pośrednie od (R, S) Zysk od (R+Kp(R), S+Kp(S)) **Razem pozycja 81**	% %	64.00 11.80	5.446 8.931	3.485 1.054 **9.990**

Tab. 3. Kalkulacja szczegółowa cen jednostkowych pozycji (wybrane wpisy) - cd.

Lp.	Pozycje kosztorysowe	Nazwa	Uproszczone	Wartość zł	Jedn. miary	Ilość jedn.	Wskaźnik na jednostkę zł	Udział procentowy
1	2	3	4	5	6	7	8	9
1	1–30	System sygnalizacji włamania i napadu		44327.95				10.06%
2	31–44	System kontroli dostępu		129304.45				29.33%
3	45–69	System sygnalizacji pożarowej		117503.93				26.65%
4	70–77	System telewizji dozorowej		54036.43				12.26%
5	78–81	System integracji		16180.07				3.67%
		Razem netto		361352.83				81.97%
		VAT		79497.62				18.03%
		Razem brutto		440850.45				100.00%
		Ogółem wartość kosztorysowa robót		**440850.45**				
		W tym:						
		Wartość kosztorysowa robót bez podatku VAT		361352.83				
		Podatek VAT		79497.62				
		Słownie: czterysta czterdzieści tysięcy osiemset pięćdziesiąt i 45/100 zł						

Tab. 4. Tabela wartości elementów scalonych

Programowanie i uruchomienie systemu alarmowego

Dużo kłopotów – szczególnie inwestorom – sprawiają etapy dotyczące programowania i uruchomienia systemu alarmowego.

Zarówno wykonawca, jak i zamawiający inaczej interpretują zasady wyceny tych czynności. Realizacja oprogramowania systemu alarmowego lub integracji jest w każdym przypadku inna i wynika przede wszystkim z zastosowanej technologii oraz dokumentacji technicznej producenta sprzętu, która określa sposób programowania i przygotowania systemu do pracy adekwatnie do wymagań zawartych w projekcie technicznym.

Przy realizacji niewielkich systemów alarmowych wycena tych czynności nie ma większego wpływu na wartość kosztorysową systemu alarmowego. Problem może pojawić się wówczas, kiedy wykonawca interpretuje programowanie dosłownie, jako wycenę każdego wpisu danych do pamięci centrali alarmowej lub stanowiska zintegrowanego PC.

Programowanie należy w sposób uogólniony, w sensie wyceny kosztorysowej rozumieć jako przygotowanie programu funkcjonalno-użytkowego dedykowanego systemu alarmowego lub zintegrowanego stanowiska zarządzania dla zabezpieczanego obiektu na podstawie dostarczonego przez producenta ogólnego schematu możliwości programowych urządzenia (systemu).

Nie należy traktować programowania jak wpisywania danych do przygotowanego wcześniej programu.

Przygotowanie zintegrowanego stanowiska zarządzania

Potrzeba przygotowania zintegrowanego stanowiska zarządzania wynika z dokumentacji projektowej, uzgodnionej z inwestorem, a nie z zaleceń wykonawcy lub producenta urządzeń (systemu alarmowego).

Najprostszy system zintegrowany składa się z komputerowego stanowiska alarmowego wyposażonego w specjalistyczne oprogramowanie zarządzające systemami alarmowymi. Uwagi dotyczące interpretacji programowania autonomicznych systemów dotyczą także programowania systemu integracji.

Większą trudność może sprawić przygotowanie i programowanie systemu alarmowego pracującego w rozległej sieci LAN lub/i WAN.

Dobrą praktyką w takiej sytuacji jest przygotowanie wyceny jednego serwera zarządzającego, a później wycena pozostałych elementów wchodzących w skład zarządzania sieci z uwzględnieniem przyjętej skali powtarzalności.

Podsumowanie

Opisane metody kalkulacji systemów alarmowych opartych o szczegółowe zasady kalkulacji są zalecane tam, gdzie zależy nam na przejrzystości i kontroli technologicznej realizacji systemu alarmowego.

Wycena kosztorysowa systemu alarmowego w oparciu o katalog KNR Al-01 w większości przypadków pozwala szczegółowo określić wartość kosztorysową systemu alarmowego.

Ze względu na wprowadzenie nowych technologii, urządzeń oraz sposobów ich instalacji niezbędne staje się przygotowanie nowelizacji i rozszerzenia KNR Al-01.

Szczególnie dotyczy to systemów alarmowych wykorzystujących technologię IP oraz pracujących w sieciach ethernetowych, wykorzystujących technologie bezprzewodowe, biometryczne czy technologie analizy wizyjnej.

Autor artykułu zwraca się do Czytelników z prośbą o przesyłanie za pośrednictwem Redakcji wszelkich konstruktywnych uwag dotyczących katalogu KNR Al-01, które będą pomocne przy przygotowywaniu nowej, rozszerzonej wersji omawianej publikacji.

DR INŻ. ANDRZEJ WÓJCIK

ALBERT + ULISSE

Zespół, który zwycięża.

Videotec dołączył do grona zwycięzców.
Zapewniamy najwyższy poziom bezpieczeństwa!

Kluczem do sukcesu jest pełna integracja oraz perfekcyjna komunikacja pomiędzy precyzyjnymi, szybkimi głowicami ULISSE a zbudowanymi w oparciu o najnowsze technologie sterownikami ALBERT.

Skonfigurowany w ten sposób system monitoringu wizyjnego stanowi niezwykle skuteczne i niezawodne rozwiązanie problemów, występujących podczas dozoru dużych przestrzeni otwartych oraz obiektów o specjalnym znaczeniu.

TÜV NORD ISO 9001

HEADQUARTERS ITALY
T. +39 0445 697411
info@videotec.com

FRANCE
T. +33 2 32094900
info@videotec-france.com

UK / IRELAND
T. +44 01353 775438
uksales@videotec.com

U.S.A. / CANADA
T. +1 973 5950788
usasales@videotec.com

ASIA PACIFIC
T. +852 2333 0601
info@videotec.com.hk

VIDEOTEC

artykuł sponsorowany

Innowacyjne rozwiązania w rejestratorach serii IN 41XX firmy INTROX

Rys. 1. Rejestrator IN 41XX

Trzy lata temu firma Janex International wprowadziła do swojej oferty produkty firmy Introx. Introx to zaawansowane urządzenia telewizji dozorowej, takie jak kamery kolorowe, dualne, w obudowach wandaloodpornych, z oświetlaczami podczerwieni o zasięgu do 50 m, a także cała gama rejestratorów cyfrowych

W niniejszym artykule chcielibyśmy zwrócić Państwa uwagę na najnowsze rejestratory cyfrowe serii IN 41XX. Rejestratory te występują w trzech wersjach – 4-, 8- i 16-kanałowej (rys. 1).

Pracują one w trybie hexaplex (jednoczesne nagrywanie, wyświetlanie, odtwarzanie, podgląd przez sieć TCP/IP, zdalna konfiguracja, zdalna archiwizacja). Rejestracja obrazu w kompresji MPEG-4 odbywa się z prędkością do 25 kl./s dla każdej kamery. Na każdy kanał wideo przypada jeden kanał audio, a dźwięk nagrywany jest z kompresją G.726. Dla każdego kanału audio można wybrać detekcję audio i ustawić poziom czułości, przy którym rejestrator zacznie nagrywać zdarzenie.

Urządzenie ma rzadko spotykaną możliwość przekazu informacji głosowej przez sieć TCP/IP w trybie „na żywo". Dodatkowo możliwa jest dwustronna komunikacja audio przez sieć TCP/IP – oprócz nasłuchiwania, co dzieje się w pomieszczeniu, w którym znajduje się mikrofon, istnieje możliwość nadania komunikatu głosowego, który będzie wysłany do głośników podłączonych do rejestratora.

W rejestratorach można zainstalować trzy dyski SATA o pojemności 1 TB każdy. Jeżeli chcemy zwiększyć bezpieczeństwo systemu lub pojemność dysków, możemy poprzez złącze IEE1394 podłączyć do rejestratora macierz dyskową RAID IN-MSATA4 firmy Introx (rys. 2). Macierz ta może pracować w trybie RAID 0, RAID 1, RAID 5 lub RAID 5+spare. Praca macierzy w jednym z trzech ostatnich trybów umożliwia odzyskanie nagranego materiału w przypadku uszkodzenia jednego z dysków (na podstawie informacji nagranych na pozostałych dyskach). Pozwala to na zainstalowanie rejestratorów Introx serii IN-41XX w systemach, które wymagają maksymalnego poziomu bezpieczeństwa nagrań.

Rys. 2. Macierz dyskowa IN-MSATA4

Wbudowana nagrywarka DVD-RW oraz dwa porty USB 2.0, do których można podłączyć pamięć przenośną (*pendrive*) lub zewnętrzny dysk, są pomocne przy archiwizacji dużej ilości nagranego materiału.

Obrazy z kamer mogą być wyświetlane na monitorze głównym (wyjście BNC bądź VGA) oraz na monitorze pomocniczym Spot (wyjście BNC). Użytkownik sam decyduje o kolejności wyświetlania kamer w podziale na monitorze głównym.

Obsługa rejestratora może odbywać się za pomocą przycisków na panelu przednim, pilota, myszy lub wyniesionej klawiatury IN-400KL (rys. 3). Klawiatura wyniesiona ma wbudowany dżojstik, który umożliwia łatwe sterowanie kamerami szybkoobrotowymi podłączonymi do rejestratora lub bezpośrednio do klawiatury.

Dzięki czterem profilom ustawień nagrywania i przypisaniu ich do harmonogramu Introx serii IN-41XX umożliwia bardzo elastyczne programowanie (rys. 4). Jeśli dodamy do tego możliwość przypisania każdej kamerze innej szybkości nagrywania (od 1 do 25 kl./s), różnej jakości i rozdzielczości obrazu oraz dowolnego trybu nagrywania (ciągłego, przy detekcji ruchu, wyzwalanego z wejść alarmowych, przy detekcji dźwięku, automatycznego), daje to nieograniczone możliwości w dopasowaniu się do indywidualnych potrzeb klienta.

Producent rozwiązał też problemy występujące w innych rejestratorach przy zmianie czasu – w rejestratorach serii IN-41XX nie tracimy nagranego materiału, gdy czas został zmieniony wstecz. Rejestrator, odtwarzając archiwum, pokazuje, że dany materiał został zapisany według starego czasu.

Każdy rejestrator może obsługiwać pięciu użytkowników, którym nadaje się różne uprawnienia, np. można ograniczać dostęp do rejestratora lub jego poszczególnych funkcji (takich jak podgląd na żywo przez sieć, odtwarzanie nagranego materiału, tworzenie kopii, dostęp do ustawień rejestratora, sterowanie kamerami PTZ, aktualizacja oprogramowania rejestratora przez sieć IP, ukrywanie kamer lokalnie i przez sieć IP).

Bardzo ważną funkcją jest informacja o braku sygnału z kamery, pojawiająca się na wyjściu przekaźnikowym, która może być wysłana na dowolny adres e-mail.

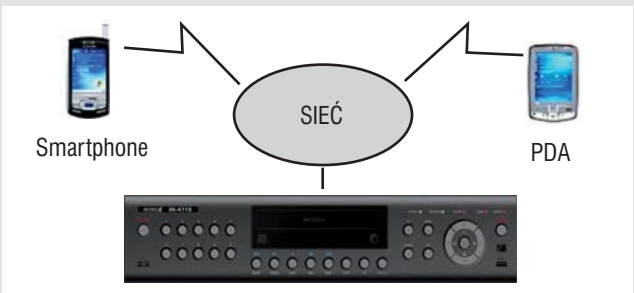
Z rejestratorami serii IN-41XX można łączyć się poprzez sieć TCP/IP, wykorzystując przeglądarkę internetową Internet Explorer bądź dedykowane oprogramowanie IN4Series-CMS.

Rys. 3. Klawiatura IN-400KL

Rys.4. Profile

Rys. 5. Wykorzystanie przeglądarki internetowej

Rys. 6. IN4Series-CMS



Rys. 7. Połączenie z rejestratorem poprzez PDA

Łącząc się za pośrednictwem przeglądarki internetowej (rys. 5) można:
- załączać przekaźniki na rejestratorze, uruchomić dwukierunkowy tor audio,
- sterować kamerami szybkoobrotowymi PTZ – wyzwalać presety, uruchamiać dwie trasy patrolowe, ustawić prędkość PTZ itp.,

System	Linux
Kompresja	wideo – MPEG-4, audio – G.723
Prędkość wyświetlania	25 kl. @ 704 x 576 na kamerę
Prędkość nagrywania	25 kl./s @ 352 x 288 na kamerę
Rozdzielczość nagrywania	352 x 288, 704 x 288, 704 x 576
Pojemność HDD	3 dyski SATA, maks. 3 TB
Archiwizacja	2 x USB 2.0, sieć IP
Audio	16 wejść RCA/1 wyjście RCA (IN-4116) 8 wejść RCA/1 wyjście RCA (IN-4108) 4 wejścia RCA/1 wyjście RCA (IN-4104)
Wejścia wideo	16 x BNC (IN-4116) 8 x BNC (IN-4108) 4 x BNC (IN-4104)
Wyjścia wideo	wyjścia przelotowe kamer 16 (8, 4) x BNC monitor główny 1 x BNC, 1 x VGA monitor pomocniczy (SPOT) 1 x BNC
Wyjścia przekaźnikowe	4 x BNC (IN-4116) 2 x BNC (IN-4108) 1 x BNC (IN-4104)
Obsługa	panel przedni, mysz USB 2.0, pilot, klawiatura wyniesiona
Pamięć zewnętrzna	zewnętrzna macierz IEEE1394 z RAID
Sterowanie PTZ	RS232C
Aktualizacja *firmware*	sieć IP, USB
Wejścia/wyjścia alarmowe	16 wejść/4 wyjścia (IN-4116) 8 wejść/2 wyjścia (IN-4108) 4 wejścia/1 wyjście (IN-4104)
Zdalna obsługa	oprogramowanie zdalne: IN4Series-CMS, przeglądarka internetowa, PDA

Tab. 1. Parametry ogólne rejestratorów serii IN 41XX

- wyszukać nagranie i je odtworzyć,
- zmienić nastawy rejestratora.

Oprogramowanie IN4Series-CMS jest narzędziem, które oprócz funkcji dostępnych z poziomu przeglądarki umożliwia m.in. jednoczesne połączenie z 4096 rejestratorami i 65536 kamerami, a na monitorze może być wyświetlany obraz z 64 kamer jednocześnie (rys. 6).

Operator może sam zmieniać elementy graficzne programu, takie jak np. grubość linii podziału, kolor, czcionka opisu kamer. Znajduje się tu również funkcja wyskakujących okienek, które są wyświetlane w chwili zaistnienia określonego zdarzenia, np. włączenia lub wyłączenia nagrywania, detekcji ruchu, aktywacji wejścia alarmowego, detekcji audio. Ponadto istnieje możliwość stworzenia kilku schematów ekranów z obrazami z dowolnych kamer, uzyskanymi z kilku rejestratorów. Zapisanie tych podziałów pod różnymi nazwami pozwala na szybkie wywołanie wyświetlania żądanego ekranu. Można jednocześnie wyświetlać dwa różne podziały na dwóch monitorach podłączonych do tego samego komputera (monitor główny + monitor pomocniczy) lub stworzyć system wyświetlania, gdzie na jednym monitorze podłączonym do komputera wyświetlane są kamery w podziale np. 1+7, 4x4 czy 8x8, a drugi monitor jest pomocniczy i wyświetlane są na nim obrazy z kamer w przypadku zaistnienia alarmu.

Bardzo istotną i innowacyjną funkcją rejestratorów Introx serii IN-41XX jest możliwość łączenia się z rejestratorami za pomocą PDA (rys. 7).

Opisane powyżej nowe rejestratory serii IN 41XX dają bardzo duże możliwości instalatorom i użytkownikom. Ich proste i przejrzyste menu oraz przystępna cena stawiają je wysoko w porównaniu z innymi obecnie dostępnymi na rynku rejestratorami.

Grzegorz Matulka
Janex International

PROMOCJA SEZONOWA
JESIEŃ 2008

GANZ

~~600 zł~~
nowa cena cennikowa:
520 zł

Kamera ZC-D2039PHA

- cyfrowa funkcja Day/Night
- rozdzielczość pozioma 480 TVL
- obiektyw 3 - 9 mm z przysłoną DC - zasilanie 12VDC/24VAC

~~970 zł~~
nowa cena cennikowa:
850 zł

Kamera ZC-DT2312PHA-IR

- mechaniczna funkcja Day/Night
- rozdzielczość pozioma 480 TVL
- obudowa wandaloodporna IP66
- obiektyw 3.3 – 12 mm z pełną korekcją IR
- oświetlacz IR 18 x LED, długość fali 850 nm
- zasilanie 12VDC/24VAC

3 lata gwarancji

Rejestratory z serii DIGIMASTER (model 8 i 16 kanałowy)

- obsługa dysków wewnętrznych maks. 3 x 750GB
- nagrywarka DVD oraz 3 porty USB 2.0
- kompresja obrazu MPEG4 w rozdzielczości 4CIF
- 4 kanały audio w każdym modelu
- dwukierunkowa transmisja audio poprzez sieć LAN
- 4 niezależne wyjścia monitorowe SPOT + wyjścia VGA i BNC
- ponad 30 zaimplementowanych protokołów PTZ
- sterowanie wieloma rejestratorami za pomocą pilota lub konsoli ZCA-SC201

Monity LCD z serii ECO (model 17 i 19 cali)

- rozdzielczość pozioma 500 TVL
- lekkie, łatwe w montażu i pozycjonowaniu
- jasność: 300cd/m2, kontrast: 800:1
- menu OSD wyświetlane na ekranie monitora
- szybki czas reakcji matrycy LCD ~ 1/4 ms
- przelotowe wyjście BNC

DR8N-DVD ~~4000~~ zł **3200 zł**
DR16N-DVD ~~4900~~ zł **3900 zł**

ZM-L217E ~~1800~~ zł **1300 zł**
ZM-L219E ~~2100~~ zł **1600 zł**

produced by CBC

Pełna oferta promocyjna dostępna u Dystrybutorów CBC

www.cbcpoland.pl

artykuł sponsorowany

Termowizja

– widzieć tam, gdzie wzrok nie sięga

Kamera C-Allview Thermal jest połączeniem dwóch uzupełniających się kamer: kamery termowizyjnej z 7-krotnym zoomem cyfrowym, której zadaniem jest wykrycie zagrożenia w obszarze do 1000 m, nawet w skrajnie niekorzystnych warunkach atmosferycznych i oświetleniowych, oraz kamery z torem optycznym, wyposażonej w 36-krotny zoom optyczny, służącej do weryfikacji ewentualnego zagrożenia

Zasada działania kamery termowizyjnej

Działanie kamery termowizyjnej C-Allview Thermal oparte jest na detekcji energii fal elektromagnetycznych w zakresie 7–14 μm (daleka podczerwień). Jest to poziom promieniowania emitowany przez każde ciało fizyczne w temperaturach od ok. 0 do 600°C.

Podstawowym elementem każdej kamery termowizyjnej jest detektor promieniowania podczerwonego. Jest to element, który odróżnia te kamery od kamer wideo. Otóż przetworniki CMOS czy CCD stosowane w kamerach wideo detekują fotony promieniowania widzialnego (lub też bliskiej podczerwieni pochodzącej z oświetlaczy IR) które po odbiciu od obserwowanego przedmiotu docierają do detektora. Kamera termowizyjna wyposażona jest natomiast w detektor mikrobolometryczny, którego zadaniem jest wykrycie temperatury docierającego promieniowania cieplnego. Jak wynika z doświadczenia Herschela, promieniowanie podczerwone jest promieniowaniem „cieplejszym" niż promieniowanie widzialne (rys. 2), czyli posiada większą energię i można je wykrywać z większych odległości niż promieniowanie widzialne.

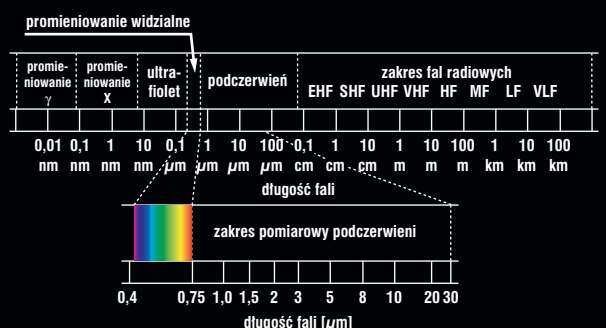
Ze względu na właściwości transmisyjne fal elektromagnetycznych w kamerach termowizyjnych zastosowanie znajdują zwykle obiektywy germanowe. Dzieje się tak, ponieważ german bardzo dobrze transmituje promieniowanie cieplne, filtrując zarazem zakres widzialny promieniowania. Oferowane przez CBC kamery termowizyjne możemy sklasyfikować pod względem zastosowanych obiektywów. Są trzy rodzaje kamery C-Allview Thermal:

- o poziomym kącie widzenia 12° i zasięgu ok. 1000 m (ogniskowa 75 mm),
- o poziomym kącie widzenia 25° i zasięgu ok. 300 m,
- o poziomym kącie widzenia 50° i zasięgu ok. 100 m.

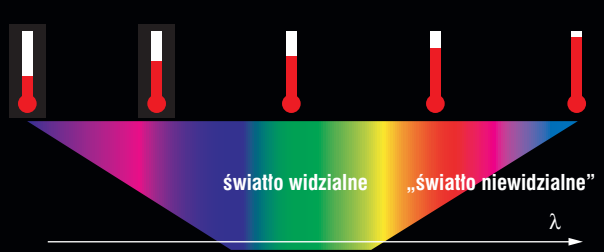
Parametry kamery z torem optycznym pozostają niezmienne w wyżej wymienionych modelach kamery C-Allview Thermal.

C-Allview Thermal

Każda kamera posiada rozbudowane, aczkolwiek intuicyjne menu. Wykorzystując zaimplementowane funkcje, można m.in. włączyć/wyłączyć koloryzację obrazu termicznego. Co więcej, można dowolnie regulować przedziały temperatur odwzorowywanych przez poszczególne barwy. Jest również możliwość pomiaru temperatury w danym obszarze. Poza tym, dzięki zastosowaniu dwóch torów wizyjnych, istnieje możliwość jednoczesnej obserwacji obrazu z kamery termowizyjnej i z kamery z torem optycznym. C-Allview Thermal oferuje dowolne przełączanie pomiędzy obserwowanymi kanałami wizyjnymi oraz wybór kamery (głównej), która ma być sterowana przez operatora.



Rys. 1. Widmo promieniowania elektromagnetycznego



Rys. 2. Temperatura promieniowania elektromagnetycznego. Temperatura promieniowania podczerwonego jest wyższa od temperatury promieniowania widzialnego

Rys. 3. Z lewej: Porównanie kamery termowizyjnej i kamery standardowej podczas obserwacji obszarów przy dużym oświetleniu
Z prawej: Porównanie kamery termowizyjnej i kamery standardowej podczas obserwacji obszarów zadrzewionych

Oprócz opisanych już cech kamera ta jest wyposażona w wandaloodporną obudowę wykonaną z silnie anodowanego, proszkowanego aluminium w celu uodpornienia na zadrapania, utlenianie oraz skutki kontaktu z rozpuszczalnikami. Użycie tych materiałów sprawia, iż kamera jest przystosowana do pracy w nieprzyjaznym środowisku. Wymienna frontowa szyba wykonana jest z hartowanego szkła i posiada zainstalowaną fabrycznie wycieraczkę, która skutecznie usuwa zanieczyszczenia oraz zgromadzoną wodę. Szyba jest odporna zarówno na fizyczny atak rzuconym przedmiotem, jak również na atak balistyczny.

Bardzo istotną zaletą kamery jest obecność modułu PTZ. Kamerą można precyzyjnie sterować nawet przy maksymalnym zbliżeniu. Istnieje również możliwość pochylenia głowicy, co całkowicie niweluje strefę martwą obserwacji, występującą np. przy montażu na słupie.

Rys. 4. Porównanie kamery termowizyjnej i kamery standardowej podczas obserwacji przy ograniczonej widoczności, w trudnych warunkach atmosferycznych

Zastosowanie

Opisane cechy kamery C-Allview Thermal powodują, że ma ona bardzo szerokie zastosowanie nie tylko w systemach bezpieczeństwa.

Jednakże ze względu na swoją wandaloodporną budowę jest ona przeznaczona głównie do instalacji w systemach ochrony życia i mienia. Można ją stosować do monitoringu rozległych terenów, obszarów o słabej lub całkowitym braku widoczności dla tradycyjnych kamer, w terenach zalesionych, w transporcie, w przemyśle itd.

Istnieje również możliwość sprzężenia kamery C-Allview Thermal z systemem radarowym i stworzenia inteligentnego systemu detekcji i śledzenia obiektu, działającego w każdych warunkach atmosferycznych.

Robert Mędrzycki
CBC Poland

artykuł sponsorowany

Nowe produkty IP z Pelco

Artykuł zawiera informacje o zapowiadanej wcześniej kamerze uchylno-obrotowej Spectra Mini IP. Przedstawiam także informacje o technologii Sarix i nowych kamerach megapikselowych Pelco, które sprzedawane będą w przyszłym roku

Spectra Mini IP

Zapowiadana na czwarty kwartał 2008 Spectra Mini IP pojawiła się w sprzedaży już we wrześniu. Jest to kolorowa kamera uchylno-obrotowa, przeznaczona do pracy wewnątrz pomieszczeń. Typowe miejsca stosowania Spectry Mini IP to biura, hotele, supermarkety i stacje benzynowe. Ponieważ zakres temperatur pracy jest szeroki: od 0°C do 50°C, kamera może być instalowana także w magazynach i garażach.

Spectra Mini IP

Moduł kamerowy umożliwia dziesięciokrotne optyczne i ośmiokrotne cyfrowe powiększenie. W pamięci kamery mogą być zapisane 64 ujęcia, które są wybierane z dokładnością 0,5°, oraz jedna trasa obserwacji. Maksymalna szybkość obrotowa kamery to 140°/s, a szybkość uchyłu w pionie – 80°/s.

Spectra Mini IP może być instalowana na powierzchni sufitu stałego lub wpuszczona w sufit podwieszany. Dostępny jest opcjonalny uchwyt ścienny i wysięgnik. Do wyboru jest biała lub czarna obudowa oraz przeźroczysty lub przyciemniony klosz kopuły. Kamera jest przystosowana do zasilania w standardzie PoE lub napięciem zmiennym 24 V z zewnętrznego zasilacza – na przykład serii MCS.

Spectra IV IP

Serwer wideo w kamerze może wysyłać strumienie wideo w formacie MPEG4 i MJPEG. Przeglądarki internetowe Internet Explorer i Mozilla Firefox umożliwiają odbiór obu typów strumieni. Przy kodowaniu MJPEG strumień wideo zawiera maksimum 15 obrazów/s, a przy MPEG4 – 25 obrazów/s w rozdzielczości 4CIF (704x576), PAL. Rejestratory sprzętowe lub oprogramowanie, które ma zaimplementowany protokół IP Pelco, mogą odbierać strumień MPEG4 w rozdzielczości 4CIF, 2CIF, CIF lub QCIF i wybraną liczbę obrazów na sekundę. Strumień danych dla rozdzielczości 4CIF przy 25 obrazów/s ma przepływność 2 Mb/s.

Odbiornikiem może być na przykład rejestrator hybrydowy serii DVR5100 lub sieciowy Integral Digital Sentry NVR, opisany w pierwszej części artykułu. Na liście producentów oprogramowania, którzy wprowadzili protokół kamer IP Pelco, znajdują się takie firmy, jak Milestone Systems, ObjectVideo, OnSSI, Plustek Inc., Visual Defence i Lenel Systems International Inc.

Technologia Sarix

Podczas targów ASIS, które odbyły się w dniach od 15 do 17 września w Atlancie (USA), firma Pelco zaprezentowała po raz pierwszy kamery megapikselowe, wykorzystujące opracowaną przez siebie technologię Sarix. Według zapowiedzi pierwsze modele kamer megapikselowych i obiektywów serii 13M będą sprzedawane w drugim kwartale 2009 roku. Początkowo dostępne będą kamery w obudowie typu *box*, pracujące w rozdzielczościach: 3.1 Mp (2048x1536), 2.1 Mp 1920x1080), 1.3 Mp (1280x1024) oraz 0.5 Mp (800x600). Następnie, w kolejnych miesiącach, do sprzedaży wprowadzane będą kamery kopułkowe do zastosowań zewnętrznych i wewnętrznych, w wersjach kolorowej i dzień/noc.

Zadaniem konstruktorów Pelco było stworzenie kamer o rzetelnym odwzorowaniu kolorów i wysokiej czułości, umożliwiającej pracę przy słabym oświetleniu. Nowe, specjalnie zaprojektowane obudowy doskonale komponują się z nowoczesną

aranżacją wnętrz we współczesnych budynkach. Kamery mogą być zasilane w standardzie PoE lub napięciem zmiennym 24 V. Dla ułatwienia strojenia wyposażone są w serwisowe wyjścia wizyjne. Wbudowany czytnik kart pamięci w standardzie mini-SD pozwala na lokalny zapis materiału wideo w kamerze. Procesor kamery koduje wideo w standardach H.264, MJPEG i MPEG4, co umożliwia współpracę z różnymi systemami rejestracji. Będzie obsługiwał także algorytmy do analizy obrazu. Funkcja QoS zastosowana w kamerze pozwala użytkownikowi kontrolować wykorzystanie dostępnego pasma transmisji. Dodatkowo możliwe jest zabezpieczenie transmisji pakietów wideo przez sieć dzięki wykorzystaniu technologii szyfrowania SSL/TLS.
Technologia Sarix EP (*Extended Platform*) jest stosowana w modelach o matrycy 2.1 megapikseli. Procesor kamery ma większą wydajność, co pozwala stosować oprogramowanie do analizy obrazu przy dużej liczbie obrazów/s. Docelowo klienci będą mogli stosować również programy analityczne innych producentów, na przykład firmy ObjectVideo. Producenci oprogramowania współpracujący z Pelco otrzymują dokumentację API do kamery i systemu analizy obrazu.

W przyszłym roku wprowadzona zostanie na rynek zupełnie nowa platforma sprzętowa do rejestracji i wizualizacji wideo z kamer megapikselowych.

Rejestratory hybrydowe serii DX8100

Obecnych użytkowników serii DX8100 ucieszy na pewno wiadomość, że w pierwszym kwartale 2009 mają zostać wprowadzone do sprzedaży rejestratory z nowym oprogramowaniem. DX8100 w wersji 2.0 stanie się rejestratorem hybrydowym. Przykładowo model DX8116 będzie mógł obsłużyć 16 kamer analogowych i 16 kamer IP, a model DX8124 – 24 kamery analogowe i 8 kamer IP. Obsługiwane będą kamery IP produkcji Pelco i firmy Axis Communications. Korzystanie z kamer IP nie będzie wymagało zakupu licencji. Dodatkowo rejestrator będzie umożliwiał podłączenie zewnętrznych systemów zapisu poprzez interfejs USB 2.0. Kolejną nowością będzie opcja startu systemu operacyjnego rejestratora z karty pamięci typu SD (*Secure Digital*).
Dla przypomnienia dodam, że we wrześniu tego roku pojawiły się w sprzedaży nowe zewnętrzne macierze dyskowe serii DX8100HDDI o pojemnościach 2250 GB, 4500 GB, 6750 GB i 9000 GB, które podłącza się do DX8100 za pomocą interfejsu SCSI. Nowe macierze, podobnie jak poprzednie modele serii DX9200HDDI, współpracują tylko z modelami DX8108 i DX8116.

W Polsce produkty Pelco są dostępne w sieci partnerów firmy TAC, która jest wyłącznym przedstawicielem firmy Pelco w Polsce. Więcej informacji o kamerach IP z Pelco można znaleźć na stronie *http://www.pelco.com/IP/home.html*. Zapraszamy też na stronę TAC *http://www.tac.com/pl*.

Norbert Góra
TAC

artykuł sponsorowany

Monitory nowej generacji
dla centrów nadzoru - seria LCD 400 marki NOVUS

Fot. 1. Monitory serii LCD 400 w sali demonstracyjnej

Każdy system nadzoru wizyjnego potrzebuje interfejsu komunikacyjnego i tym ostatnim elementem służącym do zobrazowania informacji i interakcji z użytkownikiem są monitory. Do niedawna użytkownicy skazani byli na analogowe monitory typu CRT, cechujące się dużą awaryjnością i stosunkowo krótkim czasem eksploatacji lampy. Dodatkowo monitor taki stanowił znaczny koszt budowy całego systemu. Obecnie zdecydowana większość rejestratorów posiada wyjścia wizyjne VGA, pozwalające na podłączenie dowolnego monitora komputerowego. Również większość systemów nadzoru wizyjnego, zwłaszcza te małe, to systemy bez ciągłego nadzoru operatorskiego. Zaistniałe zdarzenia weryfikuje się w nich sporadycznie, stąd też mniejszą wagę przywiązuje się do jakości użytkowanych monitorów. Prawdziwym wyzwaniem dla monitorów pozostają centra monitoringu, gdzie obrazy z wielu kamer są obserwowane nieprzerwanie przez całą dobę. W takich systemach ze względu na efektywność oraz komfort pracy operatorów trzeba dołożyć szczególnej staranności przy wyborze monitora. W niniejszym artykule chciałbym zaprezentować profesjonalne monitory telewizji dozorowej serii LCD 400 marki NOVUS

Na serię monitorów składają się dwa modele o matrycy 26-calowej NVM-426LCD(A) i 32-calowej NVM-432LCD(A). Rzeczywiste wymiary aktywne matrycy wynoszą 575.769 mm (H) x 323.712 mm (V) oraz 697.6845 mm (H) x 392.256 mm (V). Oba panele posiadają panoramiczny format 16:9. Pozostałe cechy funkcjonalne, nie wynikające z typu zastosowanej matrycy, są dla obu modeli identyczne.

W monitorach zastosowane są matryce typu TFT (sterowane cienkowarstwowymi tranzystorami), charakteryzujące się bardzo szerokim kątem widzenia oraz krótkim czasem reakcji matrycy. Kąt widzenia dla obu modeli w płaszczyźnie pionowej i poziomej wynosi odpowiednio 176/176 i 178/178 stopni, pozwalając na dużą swobodę umiejscowienia stanowiska operatorskiego oraz dodatkowo na obserwację sąsiednich monitorów. Matryce TFT cechują się również wiarygodnym odwzorowaniem barw. Także problem kontrastu, który jeszcze do niedawna był dużą bolączką w przypadku matryc typu TFT, został rozwiązany. Kontrast kształtuje się na poziomie 1:2500 i 1:3000.

W monitorach zastosowano filtr grzebieniowy 3D. Jego działanie, które polega w skrócie na opóźnieniu, a następnie porównaniu i ewentualnie uśrednieniu wartości kolorów dwóch następujących po sobie linii, pozwala na zminimalizowanie poziomu szumów. Zapewnia to bardziej czysty i przejrzysty obraz o lepszej ostrości.

Matryce TFT w monitorach charakteryzują się również wysoką luminancją (jasnością) o wartości 450 cd/m^2 i 500 cd/m^2, co przy podanych powyżej wartościach kontrastu zapewnia wysokiej jakości obraz. Dodatkowo, mimo wysokiej luminancji, zredukowano problem świecącej czerni, czyli prawidłowego odwzorowywania koloru czarnego, wynikający z przenikania oświetlenia tylnego mimo blokującego ustawienia cząsteczek ciekłych kryształów.

Charakteryzując matryce monitorów serii LCD 400, musimy również odnieść się do czasu odpowiedzi matrycy. Dla systemów monitoringu parametr ten ma ogromne znaczenie ze względu na często stosowane w takich systemach kamery szybkoobrotowe. Im krótszy czas odpowiedzi, tym mniejsze smużenie przemieszczających się w obrazie obiektów lub całego obrazu w przypadku obrotu modułu kamery szybkoobrotowej. Czas przejścia, czyli czas zapalenia się, wygaszenia i ponownego zapalenia piksela szary – biały – szary, dla matryc wynosi odpowiednio 6.5 oraz 8 ms, gwarantując komfortowe warunki pracy z kamerami obrotowymi.

O dużej przydatności monitora w centrach monitoringu decydują typy wejść wideo oraz ich liczba. Monitor posiada cztery przelotowe wejścia BNC, jedno wejście S-Video, jedno wejście VGA oraz wejście komponent YPbPr. Możliwe jest równoczesne wyświetlanie obrazu głównego (BNC, S-Video, VGA, YPbPr) oraz dodatkowo, z prawej lub lewej strony, czterech obrazów z wejść BNC. W przypadku podłączenia komputera umożliwia to pracę z oprogramowaniem przy jednoczesnym lokalnym nadzorze wizyjnym.

Monitor posiada również funkcję multipleksera dla wejść analogowych BNC. Umożliwia wyświetlanie obrazów podłączonych do wejść w podziale 2x2 lub sekwencyjne ich przełączanie ze zdefiniowanym czasem. Dodatkowo w multiplekser zostały wbudowane funkcje detekcji ruchu z regulowaną czułością oraz możliwością wyświetlenia aktywnej kamery na monitorze głównym w trybie pełnoekranowym, funkcja ukrywania kamer, utraty sygnału, a także rejestr zdarzeń systemowych. Monitor posiada wbudowane wejście i wyjście alarmowe (NO lub NC). Pamięć Flash w monitorze pozwala na lokalną rejestrację do 60 obrazów. Multiplekser posiada także wejście/wyjście sygnału do podłączenia jednokanałowych rejestratorów cyfrowych w celu ciągłej rejestracji podłączonych sygnałów wizji.

Menu ekranowe monitora jest wielojęzyczne, wyświetlane m.in. w języku polskim. Dostęp do menu może wymagać autoryzacji czterocyfrowym hasłem. Dodatkowo administrator może ustanowić blokadę wszystkich klawiszy na panelu czołowym monitora prócz klawisza „MENU".

Monitor pozwala na regulację parametrów wyświetlanego obrazu w przypadku każdego typu wejścia. Zmiany dotyczą zarówno okna głównego, jak i podokien bocznych.

Fot. 2. Układ ekranu głównego oraz czterech okien wyświetlanych z boku

Identyczne ustawienia menu, obejmujące kontrast, jasność, kolor, odcień oraz ostrość, są realizowane również dla pozostałych wejść wideo: PC i komponent. Dodatkowo możliwa jest regulacja obrazowania krawędzi w zależności od typów obserwowanych scen.

Wszystkich ustawień monitora można dokonać z poziomu przycisków panelu czołowego lub z poziomu pilota zdalnego sterowania, po uprzednim zdefiniowaniu numeru ID monitora.

Monitor został wyposażony w dwa wbudowane głośniki o mocy 5 W z regulacją głośności w menu, a także w dwa liniowe wejścia mikrofonowe.

Monitory wyróżniają się solidną metalową obudową w kolorze srebrnym. Umożliwiają montaż uchwytów w standardzie VESA 100, ale ze względu na wagę (model NVM-432LCD(A) waży 18,5 kg) zaleca się stosowanie niestandardowych uchwytów o większym rozstawie i odpowiedniej nośności.

Praca człowieka w centrum monitoringu coraz częściej wspomagana jest zaawansowanymi systemami analizy obrazu. Niemniej jednak to człowiek jest najważniejszym elementem systemu. Praca w centrum operatorskim wymaga dużej koncentracji przez dłuższy okres czasu. Wysokiej jakości monitory do zobrazowania informacji są jednym z najważniejszych elementów komfortowej i efektywnej pracy operatorów.

Patryk Gańko
Novus Security

NOVUS®
Profesjonalne rozwiązanie dla systemów CCTV

RASplus

wspólny SOFTWARE dla wszystkich serii!

rejestratory cyfrowe serii 5100, 5500, 5800

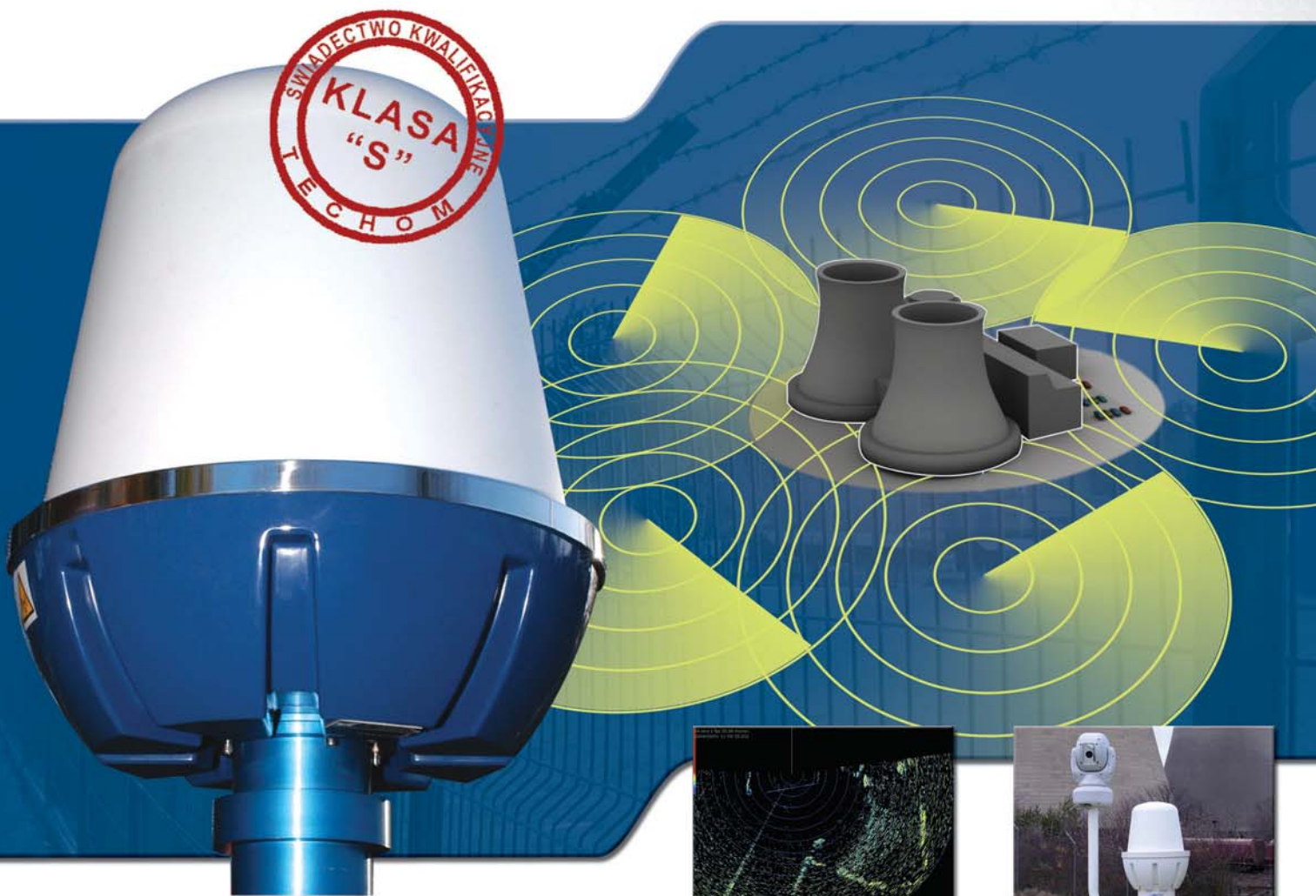
- W komplecie profesjonalny program RASplus do obsługi, zarządzania, zdalnej konfiguracji i wizualizacji obiektów za pomocą map
- Autodiagnostyka - automatyczne sprawdzanie poprawności procesów systemowych, procesu rejestracji, stanu dysków twardych S.M.A.R.T, wejść/wyjść alarmowych etc.
- Rozbudowany harmonogram nagrań
- Zaawansowany algorytm detekcji ruchu oraz detekcji obiektu (NV-DVR5800/DVD)
- Integracja obrazu z danymi tekstowymi z urządzeń typu: bankomat, kasa fiskalna, kontrola dostępu itp.
- Regulacja pasma oraz jakości obrazów transmitowanych w sieci
- Zaawansowane sposoby wyszukiwania nagrań, w tym wyszukiwanie zmian w treści obrazu
- Synchronizacja czasu systemowego

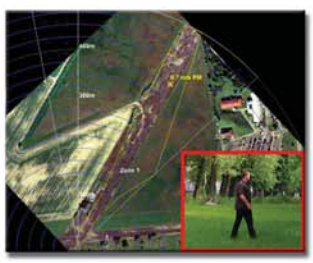
Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

KABE

WYZNACZAMY NOWE GRANICE OCHRONY





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

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

PHISHING

polowanie na łatwowiernych

(część II)

W drugiej części artykułu zostaną omówione różne odmiany *phishingu*[1], takie jak *spear phishing*, *whaling* czy *man-in-the-middle*. Ponadto przedstawione zostaną działania, jakie należy podjąć w przypadku podejrzenia, iż otrzymana wiadomość e-mail wykorzystywana jest do procedery *phishingu*, oraz sposoby zabezpieczenia się przed tym procederem

Przy tradycyjnej formie *phishingu* jego ofiarami stają się przypadkowi użytkownicy Internetu, którzy otrzymują spreparowaną wiadomość e-mail (wysyłaną do tysięcy adresatów poczty elektronicznej), lub ci, których komputery – przy okazji przeglądania stron internetowych lub instalacji oprogramowania niewiadomego pochodzenia – zostaną przypadkowo zarażone wirusem, którego przeznaczeniem jest realizacja procederu *phishingu*. Nieco inaczej działania przestępców realizowane są w sytuacji, gdy mamy do czynienia z jedną z odmian *phishingu*, nazywaną *spear phishingiem*. Przy tego rodzaju procederze działania przestępców nakierowane są na ściśle sprecyzowaną grupę użytkowników systemów informatycznych, takich jak konkretni klienci danego banku lub użytkownicy/administratorzy konkretnego systemu komputerowego w danej firmie. Celem takiego ataku jest zdobycie poufnych informacji umożliwiających przestępcom przejęcie kontroli nad konkretnym systemem lub kontem bankowym, do którego uprawnienia dostępu posiada kilka osób. Zanim nastąpi próba pozyskania poufnych informacji, np. za pośrednictwem wysyłki odpowiednio spreparowanych wiadomości e-mail, przestępcy muszą przeprowadzić swego rodzaju rozpoznanie i zdobyć szczegółowe informacje na temat grupy użytkowników, na którą ma zostać przypuszczony atak. W tym celu muszą wcześniej pozyskać ich dane osobowe, adresy e-mail, numery telefonów, wiedzę na temat posiadanych przez nich poziomów uprawnień w przypadku przygotowywania się do przejęcia kontroli nad danym systemem informatycznym. Informacje te gromadzone są przy wykorzystaniu socjotechniki stosowanej w różnych kanałach komunikacji z ofiarą. Następnie, po skutecznie przeprowadzonym etapie rozpoznania, wiadomości e-mail wysyłane przez przestępców są adresowane do konkretnych użytkowników, do których nadawca zwraca się z imienia i nazwiska, a treść wiadomości może sugerować, iż nadawca doskonale zna adresata. Niestety przy tego rodzaju ataku, do którego przestępcy przygotowują się z ogromną starannością, bardzo trudno wykryć oszustwo i jedyne, na czym można polegać, to własny zdrowy rozsądek i intuicja.

Inną odmianą *phishingu* jest *whaling*, określany mianem polowania na „grube ryby". W tym przypadku adresatami spreparowanych wiadomości są szefowie firm, biznesmeni lub wysoko postawieni urzędnicy państwowi, którzy posiadają dostęp do poufnych informacji, za które wielu jest w stanie zapłacić ogromne sumy pieniędzy. Odsyłacze umieszczone w elektronicznej przesyłce pocztowej kierują czytelnika korespondencji na stronę, z której komputer ofiary zostaje automatycznie zainfekowany niepożądanym oprogramowaniem – trojanami. Trojany takie – w sposób niewidoczny dla użytkownika – przesyłają następnie informacje o wykonywanych na komputerze ofiary ataku czynnościach na serwery zarządzane przez przestępców, dzięki czemu mogą oni wejść w posiadanie bardzo ważnych danych.

Na atak typu *phishing* jesteśmy narażeni nie tylko w sytuacji, gdy korzystamy ze stałego, kablowego połączenia z siecią. Rozwój sieci bezprzewodowych sprawia, że w coraz większej liczbie miejsc możemy skorzystać z bezpłatnego dostępu do Internetu. Gdy uruchomimy prywatnego laptopa na lotnisku czy w centrum handlowym, nierzadko możemy natknąć się na możliwość zalogowania się do niezabezpieczonego punktu dostępowego typu *hotspot*, za pośrednictwem którego możliwe jest skorzystanie z zasobów sieci. Wykorzystując do tego celu własny sprzęt, ze świadomością posiadania na nim odpowiednich zabezpieczeń, jesteśmy przeświadczeni o bezpieczeństwie operacji, które mamy zamiar wykonać, i logujemy się na konto w banku, by sprawdzić stan własnych oszczędności. Na to tylko czekają przestępcy parający się odmianą *phishingu* zwaną *man-in-the-middle*. Niczego nie podejrzewając, nie zwracamy uwagi na sąsiedni stolik w dworcowej kawiarni, przy którym siedzi niewinnie wyglądający przystojny dżentelmen, również z włączonym laptopem i uruchomioną siecią WiFi oraz modemem GPRS, umożliwiającym dostęp do sieci dzięki usłudze

1) *Phishing (spoofing)* – w branży komputerowej, oszukańcze pozyskanie poufnej informacji osobistej, jak hasła czy szczegółów karty kredytowej, przez udawanie osoby godnej zaufania, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej (źródło: Wikipedia – przyp. red.).

oferowanej przez operatora komórkowego. Nie przeczuwając najgorszego, nie mamy pojęcia, że niezabezpieczony, darmowy *hotspot*, do którego przed chwilą zalogowaliśmy się, to tak naprawdę laptop naszego sąsiada, na którym prócz skonfigurowanej możliwości skorzystania z sieci Internet zainstalowane jest również oprogramowanie śledzące nasze działania i zapisujące podawane przez nas dane... Pomijając zalecenia podane w dalszej części artykułu, najlepszym sposobem na zabezpieczenie się przed tego typu atakiem jest niekorzystanie z podejrzanych, darmowych punktów dostępu lub przynajmniej powstrzymanie się od przesyłania poufnych informacji w czasie korzystania z otwartych punktów dostępu.

Niestety dostępnych jest coraz więcej narzędzi umożliwiających amatorom *phishingu* tworzenie własnych spreparowanych stron. Co najdziwniejsze, oprogramowanie takie jest dostępne również w sieci Internet bezpłatnie i każdy chętny może ściągnąć je sobie na własny komputer i poeksperymentować, co oznacza, że w najbliższym czasie możemy mieć do czynienia z falą mniej lub bardziej dopracowanych ataków tego typu. Niepokojące jest również to, iż w ostatnim czasie pojawiły się wykorzystywane w procederze *phishingu* trojany typu *rootkit* Mebroot, które instalują się do głównego rekordu startowego dysku (*Master Boot Record*), a uaktywniają się dopiero przy ponownym uruchomieniu komputera. Kod z *rootkita* ładowany jest do MBR jeszcze przed startem systemów antywirusowych i wiele z nich nie jest w stanie go wykryć.

Co zrobić, gdy otrzymamy pocztę, co do której mamy podejrzenia? Poniżej przedstawionych zostało kilka zasad postępowania w tego typu sytuacji.

1. Należy zgłaszać przypadki otrzymania podejrzanych wiadomości e-mail. Jeśli podejrzewamy otrzymanie wiadomości e-mail związanej z *phishingiem*, która ma na celu kradzież tożsamości, należy zgłosić ten fakt organizacji, której tożsamość została sfałszowana, czyli „podrobiona". Należy skontaktować się z nią bezpośrednio – nie odpowiadając na otrzymaną wiadomość – i poprosić o potwierdzenie. Ponadto można zadzwonić pod bezpłatny numer organizacji (jeśli istnieje) i porozmawiać z przedstawicielem działu obsługi klienta. Z reguły organizacja sama – w przypadku potwierdzenia *phishingu* – podejmuje współpracę z odpowiednimi organami (np. z policją), mającą na celu zablokowanie serwerów, na które wysyłane są informacje pozyskane wskutek tego procederu.

2. Należy zachować ostrożność, klikając łącza zawarte w wiadomościach e-mail. Łącza zawarte w wiadomościach e-mail związanych z *phishingiem* często prowadzą bezpośrednio do fałszywych witryn, z których można bezwiednie przesłać oszustom własne informacje osobiste lub finansowe. Nie należy klikać łącza zawartego w wiadomości e-mail, jeśli nie wiemy, dokąd prowadzi. Nawet jeżeli na pasku adresu wyświetlany jest właściwy adres, nie dajmy się zwieść. Oszuści mają swoje sposoby na wyświetlanie fałszywych adresów na pasku adresu przeglądarki.

3. Należy wpisywać adres bezpośrednio w pasku adresu przeglądarki lub korzystać z zakładek. Jeśli musimy zaktualizować dane swojego konta lub zmienić hasło, należy wejść na odpowiednią witrynę, korzystając z zakładki lub wpisując adres bezpośrednio na pasku adresu przeglądarki.

4. Należy sprawdzić certyfikat zabezpieczeń witryny, w której wprowadzamy informacje osobiste lub finansowe. Przed wprowadzeniem w witrynie WWW jakichkolwiek informacji osobistych czy finansowych należy sprawdzić, czy jest ona bezpieczna. W przeglądarkach internetowych sprawdzajmy stan „kłódki" – ikony w prawej, dolnej części pasku stanu lub obok paska, w którym wpisywany jest adres, potwierdzającej tożsamość przeglądanej witryny. Ikona zamkniętej kłódki oznacza, że w witrynie internetowej jest używane szyfrowanie chroniące wszystkie wprowadzane poufne informacje osobiste, takie jak numer karty kredytowej, numer PESEL czy dane dotyczące płatności. Należy zauważyć, że symbol ten nie musi występować na każdej stronie witryny, a tylko na tych, na których niezbędne jest podanie informacji osobistych. Niestety podrobić można nawet symbol kłódki! W celu zwiększenia własnego bezpieczeństwa kliknij dwukrotnie ikonę kłódki, aby wyświetlić certyfikat zabezpieczeń witryny. Nazwa podana po opcji „wystawiony dla" powinna odpowiadać nazwie witryny. Jeżeli nazwy te nie są takie same, być może jest to fałszywa, „podrobiona" witryna. Jeżeli nie ma pewności, że certyfikat jest prawdziwy, nie należy wprowadzać żadnych informacji osobistych. Dla bezpieczeństwa trzeba zamknąć witrynę.

5. Nie należy wprowadzać informacji osobistych ani finansowych w oknach podręcznych. Jedną z powszechnych metod *phishingu* jest wyświetlenie fałszywego wyskakującego okna po kliknięciu łącza w sfałszowanej wiadomości e-mail. Aby okno to wyglądało na bardziej wiarygodne, może być wyświetlane na tle okna, które użytkownik uważa za autentyczne. Nawet jeśli wyskakujące okno wygląda na autentyczne lub bezpieczne, nie należy w nim wprowadzać poufnych informacji, gdyż w takim przypadku nie ma możliwości sprawdzenia certyfikatu zabezpieczeń. Należy zamknąć okna podręczne, klikając w prawym górnym narożniku okna (przycisk „Anuluj" może nie działać w oczekiwany sposób).

6. Należy aktualizować oprogramowanie komputera, używając legalnego systemu operacyjnego, oprogramowania antywirusowego oraz zapory ogniowej (*firewall*). Trzeba pamiętać o regularnym uaktualnianiu oprogramowania. Niektóre e-maile wysyłane przez *phisherów* zawierają oprogramowanie, które bez wiedzy użytkownika śledzi zachowania w Internecie. Oprogramowanie antywirusowe, uzupełnione przez zaporę ogniową, stanowi skuteczną ochronę przed nieumyślnym otwarciem tego typu plików. *Firewall* pomaga pozostać „niewidocznym" podczas surfowania w sieci, a także blokuje wszystkie nieautoryzowane połączenia. Używanie *firewalla* jest szczególnie istotne w przypadku użytkowników łącz stałych, którzy są znacznie bardziej narażeni na ataki *phisherów*. Nie należy zapominać również o instalowaniu „łat" (z ang. *patch*), które „uszczelniają" luki w naszych systemach operacyjnych[2].

Gwarancją bezpieczeństwa jest więc zarówno przywiązywanie wagi do dbałości o bieżącą aktualizację systemu operacyjnego, systemu antywirusowego i *firewalla*, jak również kierowanie się zdrowym rozsądkiem i – podobnie jak ma to miejsce w przypadku prowadzenia samochodu osobowego – zasadą ograniczonego zaufania. A gdy pojawią się jakiekolwiek wątpliwości, zawsze można w pasek adresowy ulubionej wyszukiwarki stron WWW wpisać nazwę dowolnego banku, który w swoim portfelu usług oferuje klientom możliwość skorzystania z internetowego kanału dostępu do konta, a następnie odnaleźć tam podstawowe informacje na temat bezpieczeństwa transakcji elektronicznych...

Krzysztof Białek

2) http://www.microsoft.com/poland/athome/security/email/phishingdosdonts.mspx

STACJA MONITOROWANIA

tylko do końca roku!

SUPER CENA

8999* zł

Specjalistyczna wiedza firmy Sur-Gard oraz doświadczenie w projektowaniu odbiorników stacji monitorujących została wykorzystana do stworzenia jednego z najbardziej zaawansowanych systemów monitoringu dostępnych na rynku.

SG-SYSTEM III to rozbudowany cyfrowy odbiornik telefoniczny stosowany w profesjonalnych stacjach monitorowania alarmów włamaniowych i pożarowych, który może działać także poprzez sieć TCP/IP.

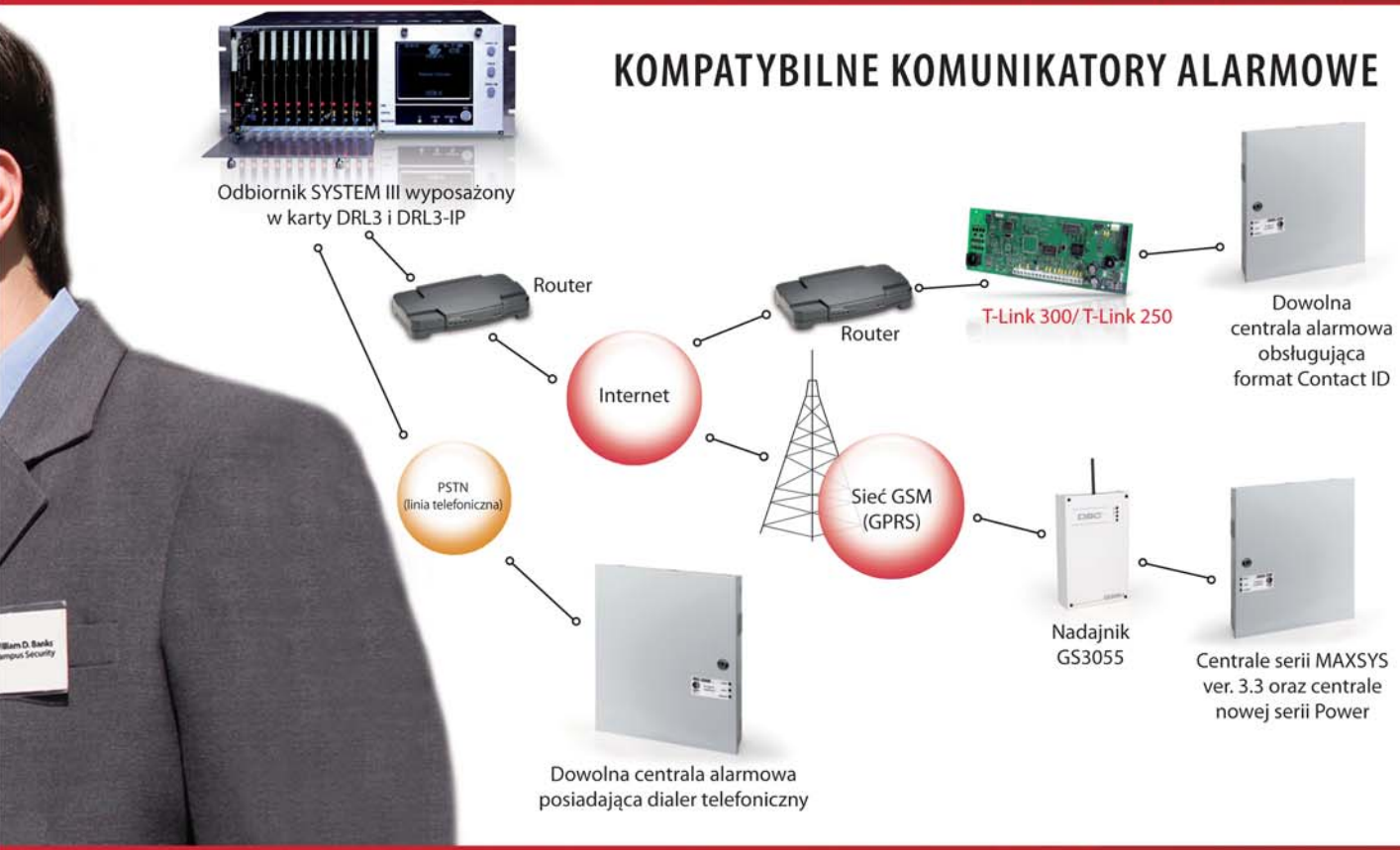
Odbiorniki *SG-SYSTEM III* firmy Sur-Gard zapewniają stacji monitorującej maksymalną wydajność i niewiarygodne oszczędności. Funkcje te możliwe są do zrealizowania dzięki zastosowaniu najwyższego poziomu zarządzania sygnałami, skróceniu czasu połączenia on-line, kontrolą nad nieautoryzowanymi połączeniami, adresowaniu TCP/IP oraz możliwości rozszerzenia systemu o dodatkowe moduły. Odbiorniki wyposażone są w duży wyświetlacz LCD dzięki czemu dostęp do opcji systemu jest prosty.

Wyłączny dystrybutor w Polsce:

AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

* cena netto, obowiązuje do 31 grudnia 2008 roku

Sur-Gard SG-SYSTEM III



Specyfikacja techniczna

- Możliwość rozbudowy do 12 kart linii (2 karty w zestawie)
- Najwyższy poziom zarządzania sygnałami redukujący czas połączenia on-line
- DNIS (Dialed Number Identification Service): usługa identyfikacji wybranego numeru
- ANI (Automatic Number Identification): automatyczna identyfikacja numeru
- Opatentowany system AHS (Automated Handshake Selection): automatyczny wybór handshake'u
- Szybkie odszukanie błędnie zaprogramowanych lub źle działających dialerów telefonicznych, jak i zakłóceń linii telefonicznych
- Upgrade systemu odbywa się poprzez flashowanie EPROMU
- Rejestr 1000 zdarzeń dla każdej karty linii (maks. 127 znaków na zdarzenie)
- 1 port równoległy, dwa porty szeregowe RS232 i złącze 10/100 BaseT
- Ciągłe monitorowanie wszystkich dróg komunikacji, zasilaczy systemowych i modułów CPM3
- Wszystkie moduły w systemie pracują indywidualnie co zapewnia nieprzerwaną pracę systemu w przypadku zmian sprzętowych lub modyfikacji oprogramowania
- Wszystkie karty mogą być wyjmowane i przekładane bez potrzeby zdejmowania napięcia zasilania
- Ciągły nadzór połączenia pomiędzy odbiornikiem a komputerem
- Szybka transmisja danych do komputera i na drukarkę zapewniająca możliwość natychmiastowej reakcji ze strony operatora
- Nadzór linii telefonicznej
- Duży i czytelny ekran LCD
- Montaż w standardowej szafie typu rack 19". Do instalacji można użyć następujących szaf rackowych: MLR2-CL, MLR2-CM, IMRAK1400 lub innych zgodnych ze standardem

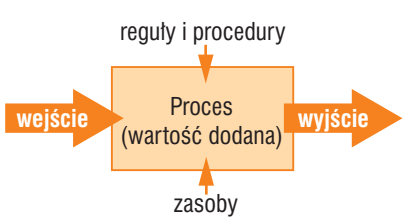
Zarządzanie ryzykiem
w działalności gospodarczej (część 2)

Kontynuując cykl artykułów w czasopiśmie *Zabezpieczenia* i odwołując się do jego pierwszej części związanej z tematyką podstaw zarządzania ryzykiem na przykładzie zarządzania bezpieczeństwem informacji, pragnę przybliżyć Państwu modele zarządzania ryzykiem oraz przekazać własne podejście do tego tematu. Zastrzegam, że jest to moje osobiste podejście do zarządzania ryzykiem, wynikające z praktyki. Zapraszam do ewentualnej polemiki wszystkich chętnych czytelników

W różnych publikacjach często spotykamy się z pojęciami tradycyjnego podejścia do zarządzania ryzykiem i podejścia zintegrowanego. W ramach tego zintegrowanego podejścia rozróżnia się rozmaite modele, np. Standard Australijsko-Nowozelandzki AS/NZS 4360, ERM COSO II, Standard Zarządzania Ryzykiem AIRMIC, Standard Brytyjski CRAMM czy Standard Organizacji FERMA oraz wiele innych. Temat ten wraz z porównaniem różnych standardów bardzo dobrze przedstawia artykuł moich kolegów pt. *Nie ma jednego sposobu zarządzania ryzykiem* W. Machowiaka i I. Stańca, zamieszczony w czasopiśmie *CFO Magazyn Finansistów* w numerze 4/07. Zachęcam Państwa do jego przeczytania.

Chciałabym przedstawić tutaj swoje podejście pozwalające odpowiedzieć na pytanie, który standard należy zastosować. Zacznijmy od tego, że zarządzanie ryzykiem jest procesem. Na rysunku 1 przedstawię schematycznie najprostszą definicję procesu[1].

Proces zarządzania ryzykiem na wejściu ma określoną sytuację zaistniałą w pewnym kontekście (obszarze), generującą ryzyko, a na wyjściu tego procesu mamy inną sytuację zmienioną o wartość dodaną, jaką może być np. ograniczenie strat czy wykorzystanie szans, czyli generujący zmodyfikowane ryzyko. Ten kontekst (obszar) to określone zasoby i reguły nimi rządzące, zgodne ze strategią działania firmy i celami biznesowymi, jakie powinny zostać osiągnięte.



Rys. 1. Graficzne przedstawienie procesu

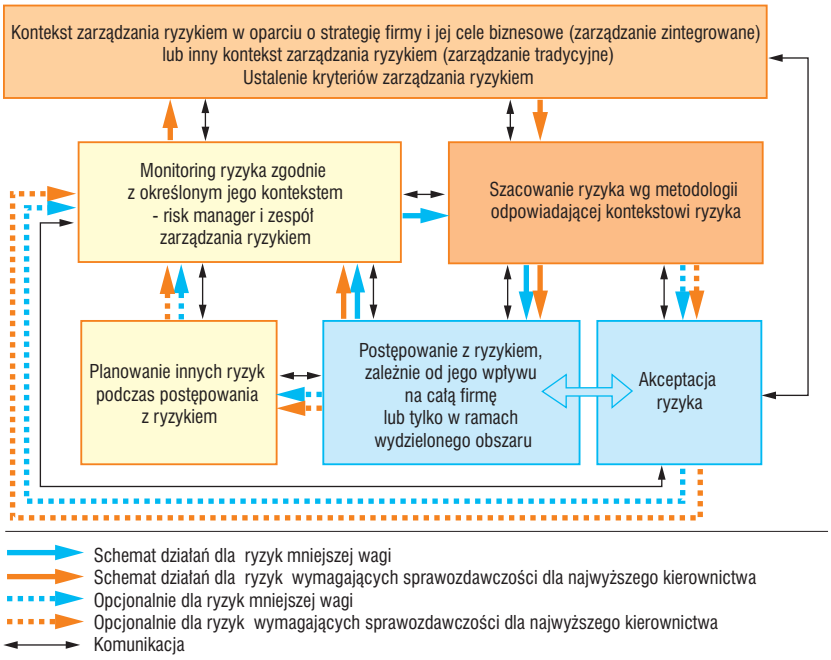
1) Jarosław Żeliński, prezentacja pt. *Czym jest i dlaczego tak ważna jest we współczesnej firmie praca grupowa*, 2007.

Według mnie na każdy istniejący w firmie proces można nałożyć reguły procesu zarządzania ryzykiem, które pozwolą tak sterować procesem, aby nic nie zakłóciło możliwości osiągnięcia celu biznesowego (zarządzanie ryzykiem negatywnym) albo aby zarządzanie ryzykiem umożliwiło zwiększenie szans firmie, która postanowiła je podjąć, a tym samym wykorzystała istniejące możliwości - szanse (zarządzanie ryzykiem pozytywnym).

Według mojej oceny każdy standard zarządzania ryzykiem posiada te same elementy i niezależnie od tego, czy zajmujemy się globalnym zarządzaniem ryzykiem w firmie i stosujemy tzw. zarządzanie zintegrowane wg wybranego standardu, czy też zarządzamy ryzykiem w określonych obszarach firmy i nie badamy wpływu występujących ryzyk na pozostałe obszary, schemat zarządzania ryzykiem jest identyczny i wszystkie standardy można doprowadzić do jednego sposobu działania. A dlaczego? Dlatego, że zarządzanie ryzykiem jest procesem składającym się z tych samych elementów.

W każdej sytuacji musimy znać strategię firmy i jej odniesienie do problemu zarządzania ryzykiem w dowolnym jej obszarze. Następnie, po określeniu kontekstu ryzyka (ten kontekst ma wpływ na to, jakie dalsze kroki będziemy wykonywać w procesie zarządzania ryzykiem, a przede wszystkim na to, jakie techniki szacowania ryzyka zastosujemy, jak będziemy z nim postępować), **przeprowadzamy długi i nieraz bardzo skomplikowany proces szacowania ryzyka**. Dopiero ryzykiem dobrze oszacowanym można prawidłowo zarządzać. A na czym polega to zarządzanie? Na właściwym sposobie jego podjęcia i monitorowania efektów tego działania, na ustaleniu kryteriów oceny ryzyka i umiejętności płynnej zmiany tych kryteriów, zależnie od rozwoju sytuacji i reakcji na dotychczasowe sposoby podjęcia ryzyka, a w uzasadnionych przypadkach na zmianie strategii firmy i jej podejścia do ryzyka. To wszystko jest możliwe tylko i wyłącznie przy zastosowaniu skutecznej komunikacji i właściwej decyzyjności na poszczególnych etapach procesu zarządzania ryzykiem. Proszę zauważyć, że rozważamy tu proces zarządzania ryzykiem, a nie ryzykami. Z tego wynika, że każdy proces w firmie może mieć na siebie nałożonych wiele procesów zarządzania ryzykiem, zależnie od tego, ile ryzyk zostało zidentyfikowanych w tym procesie.

Można by mi zarzucić, że mówię o modelu procesowym zarządzania firmą np. wg standardu ISO i o zarządzaniu ryzykiem w firmach, w których występują opisane procesy. Absolutnie tak nie jest. Proces zarządzania ryzykiem może dotyczyć obszaru działalności firmy, np. wzmiankowanego w pierwszym odcinku naszego cyklu obszaru bezpieczeństwa informacji lub obszaru związanego z bezpieczeństwem i higieną pracy pracowników, w ramach którego mamy znane wszystkim zasady BHP i wymaganą przepisami prawa ocenę



Rys. 2 . Model RMTP © Anna Słodczyk, Piotr Mąkosa

ryzyka zawodowego oraz późniejsze nim zarządzanie poprzez podejmowanie ryzyka zgodnie z obowiązującymi przepisami prawnymi. Wprowadzenie tych przepisów prawnych i kontrola ich przestrzegania jest jednym ze sposobów podjęcia ryzyka w obszarze dotyczącym bezpieczeństwa i higieny pracy pracowników. W takim przypadku określamy obszar, dla którego identyfikujemy ryzyka i nimi zarządzamy, stosując reguły zarządzania ryzykiem.

Dotychczasowe wypowiedzi można uznać za podejście tradycyjne, dziś już być może niezbyt modne, ale nadal funkcjonujące w firmach i nadal potrzebne, do momentu wprowadzenia profesjonalnego zarządzania zintegrowanego (zwanego inaczej korporacyjnym lub ERM – *Enterprise Risk Management*). A jaka jest definicja zintegrowanego zarządzania ryzykiem? Wg najpopularniejszego standardu ERM COSO II[2]:

„Zarządzanie ryzykiem korporacyjnym jest realizowanym przez zarząd, kierownictwo lub inny personel przedsiębiorstwa, uwzględnionym w strategii i w całym przedsiębiorstwie procesem, którego celem jest identyfikacja potencjalnych zdarzeń mogących wywrzeć wpływ na przedsiębiorstwo, utrzymywanie ryzyka w określonych granicach oraz rozsądne zapewnienie realizacji celów przedsiębiorstwa."

Mamy tu wyraźnie zaznaczone słowo „identyfikacja". Identyfikacja stanowi element szacowania ryzyka. Utrzymywanie ryzyka w określonych granicach to podejmowanie ryzyka na podstawie jego oszacowania, a granicami są kryteria przyjęte w strategii ustanowionej przez kierownictwo. Słowa „rozsądne zapewnienie realizacji celów przedsiębiorstwa" oznaczają takie podejmowanie ryzyk i takie ustalanie kryteriów, aby eliminować negatywne skutki ryzyk, mogące przeszkodzić w osiągnięciu celów biznesowych firmy, a także takie wykorzystywanie możliwości, aby te cele jak najlepiej zrealizować. I znów mamy tutaj proces zarządzania ryzykiem (słowo „proces" występuje w samej definicji), ale w trakcie identyfikacji i całego procesu szacowania ryzyka musimy brać pod uwagę wpływ każdego zagrożenia mogącego podnosić stopień ryzyka dla całej firmy, każdego jej procesu i każdego obszaru, a także na osiąganie przez nią ustalonych celów biznesowych. Patrząc więc przez pryzmat całej firmy, stosujemy zupełnie inne kryteria i często inne sposoby podejmowania ryzyka, ale sam proces zarządzania ryzykiem wygląda nadal tak samo.

W dzisiejszych czasach model COSO II jest najbardziej popularny, gdyż jasno odnosi się do strategii firmy i osiągania przez nią celów biznesowych, bardzo silnie opierając się na procesach kontrolnych, oraz dotyczy każdego obszaru i każdego procesu firmy, integrując ze sobą wszystkie ww. działania. Według mnie w każdym z modeli można w momencie ustalania tzw. kontekstu (obszaru) zarządzania ryzykiem zdefiniować te właśnie elementy, a kontrolę traktować jako element podejmowania ryzyka, a bardziej szczegółowo – jako sposób jego redukcji. Jednak tylko w modelu COSO II jest to wyraźnie przedstawione na schemacie słynnego sześcianu. Polecam Państwu literaturę z tego zakresu (patrz przypis nr 2).

Poniżej przedstawiam Państwu bardzo prosty model zarządzania ryzykiem – RMTP, który według mnie jest spójny z każdym modelem (standardem) zarządzania ryzykiem. Różnice pomiędzy modelami polegają na różnym zdefiniowaniu kontekstu i strategii oraz na zastosowaniu różnych metod szacowania ryzyka i różnych sposobów podejmowania ryzyka.

W kolejnej, trzeciej części omówię ten model szczegółowo, a mój kolega, współautor pierwszej części artykułu, opisze metody szacowania ryzyka.

Autorka dziękuje Piotrowi Mąkosie za merytoryczną konsultację niniejszego artykułu.

Anna Słodczyk
Risk Management Team Poland

Literatura:

1. *Nie ma jednego sposobu zarządzania ryzykiem*, w: *CFO Magazyn Finansistów*, nr 4/07.
2. Polskie tłumaczenie książki *Zintegrowany System Zarządzania Ryzykiem. Struktura ramowa* współopracowane przez ekspertów z Zespołu Zarządzania Ryzykiem PBSG i PIKW, wydanie WEMA Wydawnictwo – Poligrafia, 2007.
3. Jarosław Żeliński, prezentacja pt. *Czym jest i dlaczego tak ważna jest we współczesnej firmie praca grupowa*, 2007.
4. PN-ISO/IEC 27001:2007 System zarządzania bezpieczeństwem informacji – wymagania.
5. ISO/IEC 27005:2008 provides guidelines for information security risk management.
6. http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf
7. http://www.cramm.com/overview/howitworks.htm
8. http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tn032.pdf
9. http://www.airmic.com

2) Polskie tłumaczenie książki *Zintegrowany System Zarządzania Ryzykiem. Struktura ramowa* opracowane wspólnie przez ekspertów z Zespołu Zarządzania Ryzykiem PBSG i PIKW, wydanie WEMA Wydawnictwo – Poligrafia, 2007.

RACS ROGER ACCESS CONTROL SYSTEM

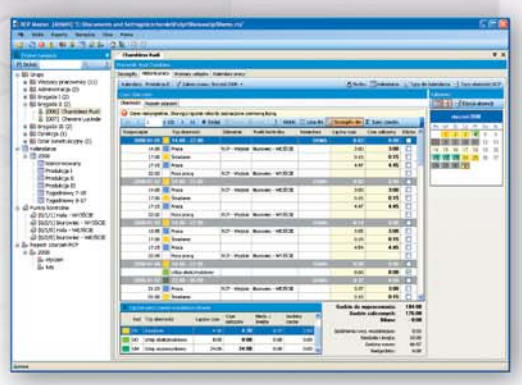
seria radius

CE

Seria Radius

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

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



RCP Master

RCP Master

Program wyposażony w przyjazny interfejs graficzny umożliwiający w łatwy sposób analizę czasu pracy/obecności w oparciu o rejestr zdarzeń zaimportowany z systemu kontroli dostępu RACS lub z pliku zewnętrznego (TXT, XML) o formacie kompatybilnym z programem RCP Master. RCP Master jest nowoczesnym typem programu, który został opracowany w środowisku Microsoft .NET i jest przeznaczony dla systemów operacyjnych Windows XP i Vista.

profesjonalna kontrola dostępu

roger®

www.roger.pl

System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001

Cz. 4. Model PDCA w procesach SZBI (ISMS)

Artykuł ten jest ostatnią częścią cyklu poświęconego zarządzaniu bezpieczeństwem informacji zgodnemu z normą ISO/IEC 27001, w której zostanie omówiony jeden z modeli zarządzania bezpieczeństwem systemów informatycznych

1. Wprowadzenie

Istnieje wiele modeli zarządzania bezpieczeństwem systemów informatycznych. Przykładowo modele zaprezentowane w arkuszu PN-I-13335 dostarczają tych pojęć, które są niezbędne do zrozumienia problematyki zarządzania bezpieczeństwem systemów informatycznych. Opisane zostaną następujące modele:

- zależności pomiędzy elementami bezpieczeństwa;
- zależności w zarządzaniu ryzykiem;
- proces zarządzania bezpieczeństwem systemów informatycznych.

W niniejszej pracy zostało omówione typowe rozwiązanie normatywne, polegające na realizacji zasady ciągłego doskonalenia, czyli realizacji cyklu Deminga, tj. PDCA[1] (*Plan-Do-Check-Act*), co odpowiada rzeczywistemu kierunkowi działań normatywnych w ostatnim okresie, zawartych w normach ISO 9001:2000, BS 7799-2:2002 i ISO/IEC 27001.

2. Wymagania funkcjonalne

Norma ISO/IEC 27001 stosuje model „Planuj – Wykonuj – Sprawdzaj – Działaj" (PDCA) , który jest stosowany do całej struktury procesów SZBI (ISMS). Na rysunku 1 przedstawiono ten model oraz pokazano, w jaki sposób ISMS przyjmuje wymagania bezpieczeństwa informacji i oczekiwania zainteresowanych stron jako wartość wejściową, a poprzez niezbędne działania i procesy dostarcza wartości wyjściowych bezpieczeństwa informacji, które spełniają te wymagania i oczekiwania.

Przykładowym wymaganiem może być takie zarządzanie informacją, że naruszenie jej bezpieczeństwa nie doprowadzi do strat finansowych w organizacji.

Natomiast oczekiwanie to na przykład odpowiednio przeszkoleni pracownicy, którzy w przypadku wystąpienia sytuacji kryzysowej ograniczą jej negatywny wpływ na instytucję.

Odpowiednie ustanowienie i zarządzanie ISMS wymaga cyklicznego podejścia, którego celem jest zapewnienie, że procedury przyjęte w danej organizacji są dokumentowane, wdrażane i w razie potrzeby doskonalone.

Przyjęcie modelu PDCA odzwierciedla także zasady określone w zaleceniach OECD, na których opiera się bezpieczeństwo systemów informatycznych i sieci. Niniejsza norma dostarcza pełnego modelu wdrożenia zasad podanych w zaleceniach, na których opiera się szacowanie ryzyka, projektowanie, wdrażanie bezpieczeństwa, zarządzanie bezpieczeństwem i ponowne szacowanie.

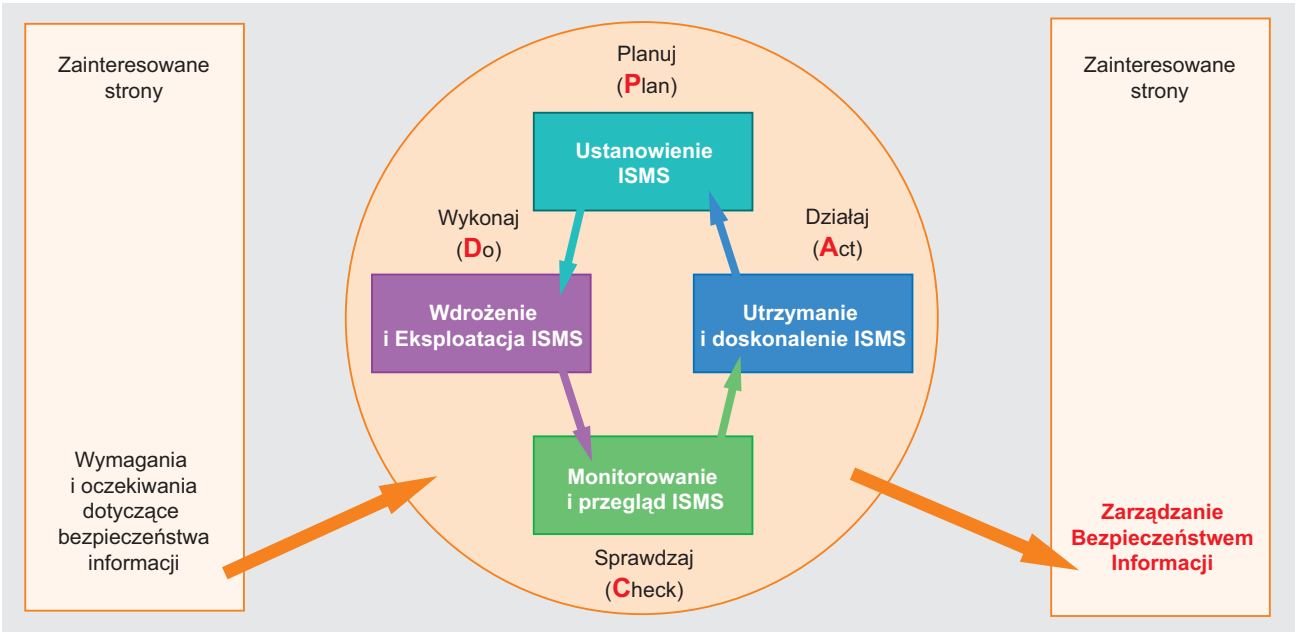
Wymagania opisane w niniejszej normie są ogólne i przeznaczone do stosowania we wszystkich organizacjach, niezależnie od typu, rozmiaru i natury biznesu.

Faza planowania

Celem fazy planowania jest ustanowienie polityki bezpieczeństwa oraz procedur dla zarządzania ryzykiem i doskonalenia ISMS. Etap ten ma zapewnić, że system zarządzania bezpieczeństwem informacji został ustanowiony prawidłowo, zidentyfikowano wszystkie rodzaje ryzyka i opracowano odpowiedni plan ich ograniczenia.

Wszelkie czynności podejmowane w ramach fazy planowania powinny być udokumentowane, by istniała możliwość ich odtworzenia i zarządzania wprowadzonymi zmianami.

1) PDCA – z ang. *Plan-Do-Check-Act* (Planuj – Wykonuj – Sprawdzaj – Działaj)



Rys. 1. Model PDCA stosowany w procesach systemu zarządzania bezpieczeństwem informacji ISMS (Information Security Management System)

Planuj – *Plan* (ustanowienie ISMS)	Ustanowienie polityki ISMS, celów, procesów i procedur istotnych dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa informacji tak, aby uzyskać wyniki zgodne z ogólnymi politykami i celami organizacji.
Wykonuj – *Do* (wdrożenie i eksploatacja ISMS)	Wdrożenie i eksploatacja polityki ISMS, zabezpieczeń, procesów i procedur.
Sprawdzaj – *Check* (monitorowanie i przegląd ISMS)	Szacowanie i – tam, gdzie ma zastosowanie – pomiar wydajności procesów w odniesieniu do polityki ISMS, celów i doświadczenia praktycznego oraz dostarczanie raportów kierownictwu do przeglądu.
Działaj – *Act* (utrzymanie i doskonalenie ISMS)	Podejmowanie działań korygujących i zapobiegawczych, bazujących na wynikach wewnętrznego audytu ISMS i przeglądzie realizowanym przez kierownictwo lub na innych istotnych informacjach w celu zapewnienia ciągłego doskonalenia ISMS.

Norma PN-I-07799-2:2005 nakłada na kierownictwo obowiązek sformułowania polityki bezpieczeństwa, za pomocą której wskazane zostaną cele i zasady postępowania w odniesieniu do bezpieczeństwa informacji. Wytyczne określające zawartość wspomnianej polityki podaje ISO/IEC 17799.

W ramach fazy planowania dokonuje się identyfikacji i szacowania rodzajów ryzyka, na jakie narażone jest organizacja. Działania te powinny być odpowiednio udokumentowane z określeniem narzędzi oraz technik zastosowanych w celu osiągnięcia prawidłowych rezultatów.

Należy ustalić akceptowalny poziom ryzyka. W przypadku zidentyfikowania ryzyka o poziomie nieakceptowanym można przyjąć różne warianty postępowania:

- zaakceptować wykryte ryzyko (działania korygujące są zbyt kosztowne lub niewykonalne ze względu na charakter procesu);
- wykonać transfer ryzyka;
- ograniczyć ryzyko do akceptowalnego poziomu.

W normie PN-I-07799-2:2005 zalecane jest tworzenie planu postępowania z ryzykiem, czyli dokumentu wskazującego czynności podjęte dla zredukowania nieakceptowanych poziomów ryzyka i implementacji odpowiednich zabezpieczeń.

Plan postępowania z ryzykiem zawiera:

- przyjętą metodę postępowania ze zidentyfikowanym ryzykiem;
- wdrożone zabezpieczenie;
- w razie potrzeby dodatkowe zabezpieczenie;
- termin wdrożenia zabezpieczeń;
- szczegółowy harmonogram pracy i zakresy obowiązków w trakcie implementacji zabezpieczeń, czyli w ramach fazy wykonania.

Faza wykonania

Na etapie wykonania ma miejsce wdrożenie i eksploatacja przyjętej polityki bezpieczeństwa oraz ustalonych zabezpieczeń i procedur. W celu zapewnienia skutecznego funkcjonowania ISMS należy przypisać odpowiednie zasoby (materialne i niematerialne) do implementacji zabezpieczeń oraz wdrożyć program uświadamiania i szkolenia pracowników w zakresie zarządzania ryzykiem i bezpieczeństwem.

W zależności od podjętych w trakcie fazy planowania decyzji dotyczących postępowania z ryzykiem należy:

- nie podejmować żadnych działań dotyczących ryzyka oszacowanego jako akceptowalne;
- wykonać transfer ryzyka (zawrzeć umowę, ubezpieczyć się, utworzyć spółkę) i upewnić się, że instytucja przejmująca ryzyko będzie zdolna zarządzać nim w sposób efektywny;
- wdrożyć zabezpieczenia zgodnie z planem postępowania z ryzykiem.

Po ograniczeniu lub przetransferowaniu ryzyka nieakceptowanego może pozostać ryzyko szczątkowe. Wdrożone mechanizmy kontrolne powinny zapewniać natychmiastową identyfikację i zarządzanie również tego rodzaju ryzykiem.

Faza sprawdzania

W fazie sprawdzania realizowany jest pomiar lub szacowanie wykonania procedur i wymogów polityki bezpieczeństwa. Działania sprawdzające mają poświadczyć, że wdrożone zabezpieczenia funkcjonują efektywnie i zgodnie z zamierzeniami, a ISMS pozostaje skuteczny. Jeśli mechanizmy zabezpieczające okażą się nieodpowiednie, należy podjąć działania naprawcze. Celem czynności korygujących jest utrzymanie spójności dokumentacji ISMS i niedopuszczenie do narażania instytucji na nieakceptowane ryzyko.

Faza sprawdzania powinna obejmować też opis procedur zarządzania i eksploatacji zabezpieczeń w ISMS oraz bieżącego przeglądu ryzyka z uwzględnieniem zmieniających się technologii, zagrożeń, podatności i wymagań biznesowych.

W zależności od rozważanego modelu PDCA w ramach fazy sprawdzania można wykorzystać następujące techniki testowania:

1. **Rutynowe sprawdzanie** – procedury wykonywane regularnie w ramach procesu biznesowego, które pozwalają wykryć nieprawidłowości będące wynikiem przetwarzania.
2. **Samokontrolujące procedury** – narzędzie umożliwiające natychmiastowe wykrycie każdego błędu pojawiającego się w trakcie wykonywania jakiegoś procesu (np. narzędzie monitorujące sieć, które powoduje uruchomienie alarmu w momencie wystąpienia defektu).
3. **Uczenie się od innych** – zbadanie, jak inne instytucje radzą sobie z określonymi problemami dotyczącymi oprogramowania technicznego i działań zarządczych.
4. **Wewnętrzne audyty ISMS** – działania wykonywane regularnie (przynajmniej raz w roku) w celu określenia poprawności funkcjonowania ISMS. Materiał dowodowy powinien potwierdzać, że:
   - polityka bezpieczeństwa jest nadal aktualna i spełnia wymagania biznesowe;
   - metodyka zarządzania ryzykiem jest odpowiednia;
   - udokumentowane procedury dotyczące ISMS spełniają zamierzone cele i są przestrzegane;
   - zabezpieczenia techniczne (np. zapory, zabezpieczenia dostępu fizycznego) są poprawnie zaimplementowane, skonfigurowane i działają zgodnie z zamierzeniami;
   - ryzyka szczątkowe są odpowiednio oszacowane i akceptowalne dla kierownictwa organizacji;
   - rekomendacje wynikające z poprzednich audytów zostały zrealizowane;
   - ISMS jest zgodny z PN-I-07799-2:2005.

   Audyty są realizowane z wykorzystaniem odpowiednio dobranej próby aktualnych zapisów i dokumentów oraz wywiadów z zaangażowanym w badany proces kierownictwem i personelem.
5. **Przeglądy wykonane przez kierownictwo** – celem tych działań jest sprawdzenie efektywności działania ISMS, zidentyfikowanie elementów wymagających udoskonalenia i podjęcie odpowiednich prac korygujących.
6. **Analiza trendów** – działania prowadzone regularnie, wskazujące obszary wymagające ulepszeń.

Faza działania

Celem fazy działania jest podjęcie odpowiednich czynności naprawczych oraz zapobiegawczych na podstawie wniosków kierownictwa wyciągniętych z przeprowadzonych w poprzedniej fazie testów. Wszystkie te działania mają prowadzić do ciągłego doskonalenia ISMS.

Według PN-I-07799-2:2005 zaleca się podejmowanie działań korygujących (lub reaktywnych) w celu eliminowania przyczyny niezgodności lub innych niepożądanych sytuacji i zapobiegania ich powtórzeniu.

Zaleca się podejmowanie działań naprawczych (lub prewencyjnych) w celu eliminowania przyczyny potencjalnych niezgodności lub innych niepożądanych sytuacji.

3. Cele stosowania zabezpieczeń i zabezpieczenia wg ISO/IEC 27001

Model Systemy Zarządzania Bezpieczeństwem Informacji został oparty o zdefiniowane w normie cele stosowania zabezpieczeń i zabezpieczenia i zawiera opisane poniżej zabezpieczane obszary działania organizacji.

1. Polityka bezpieczeństwa

– **Polityka bezpieczeństwa informacji**
Cel: sprawienie, by kierownictwo wspierało bezpieczeństwo informacji i kierowało nim zgodnie z wymaganiami biznesowymi i właściwymi przepisami prawa oraz regulacjami wewnętrznymi

2. Organizacja bezpieczeństwa informacji

– **Organizacja wewnętrzna**
Cel: zarządzanie bezpieczeństwem informacji w organizacji

– **Strony zewnętrzne**
Cel: utrzymanie bezpieczeństwa informacji należących do organizacji oraz środków przetwarzania informacji, do których mają dostęp, za pomocą których przetwarzają, komunikują się lub którymi zarządzają strony zewnętrzne

3. Zarządzanie aktywami

– **Odpowiedzialność za aktywa**
Cel: osiągnięcie i utrzymanie odpowiedniego poziomu ochrony aktywów organizacji

– **Klasyfikacja informacji**
Cel: sprawienie, by informacje uzyskały ochronę na odpowiednim poziomie

4. Bezpieczeństwo zasobów ludzkich

– **Przed zatrudnieniem**
Cel: sprawienie, by pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecią rozumieli swoje obowiązki, byli odpowiedni do wyznaczonych im ról; zredukowanie ryzyka kradzieży, naruszenia i niewłaściwego korzystania z urządzeń

– **Podczas zatrudnienia**
Cel: sprawienie, by pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecią byli świadomi zagrożeń i innych aspektów bezpieczeństwa informacji, swoich obowiązków i odpowiedzialności prawnej oraz byli wyposażeni podczas swej normalnej pracy w środki wspomagające politykę bezpieczeństwa organizacji oraz minimalizujące ryzyko błędów ludzkich

– **Zakończenie lub zmiana zatrudnienia**
Cel: sprawienie, by pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią odeszli z organizacji lub zmienili stanowisko w sposób zorganizowany

5. Bezpieczeństwo fizyczne i środowiskowe

– **Obszary bezpieczne**
Cel: zapewnienie ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w siedzibie organizacji oraz w odniesieniu do informacji

– **Bezpieczeństwo sprzętu**
Cel: zapobieganie utracie, uszkodzeniu, kradzieży lub naruszeniu aktywów oraz przerwaniu działalności organizacji

6. Zarządzanie systemami i sieciami

– **Procedury eksploatacyjne i zakresy odpowiedzialności**
Cel: zapewnienie prawidłowej i bezpiecznej eksploatacji środków przetwarzania informacji

– **Zarządzanie usługami dostarczanymi przez strony trzecie**
Cel: wdrożenie i utrzymanie odpowiedniego poziomu bezpieczeństwa informacji i dostaw usług zgodnie z umowami serwisowymi zawartymi ze stronami trzecimi

– **Planowanie i odbiór systemów**
Cel: minimalizowanie ryzyka awarii systemów

– **Ochrona przed kodem złośliwym i kodem mobilnym**
Cel: ochrona integralności informacji i oprogramowania

– **Kopie zapasowe**
Cel: zapewnienie integralności i dostępności informacji oraz środków przetwarzania informacji

– **Zarządzanie bezpieczeństwem sieci**
Cel: zapewnienie ochrony informacji w sieciach oraz ochrony infrastruktury wspomagającej

– **Obsługa nośników**
Cel: zapobieganie nieautoryzowanemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu aktywów oraz przerwom w działalności biznesowej

– **Wymiana informacji**
Cel: utrzymanie bezpieczeństwa informacji i oprogramowania wymienianego wewnątrz organizacji oraz z każdym podmiotem zewnętrznym

– **Usługi handlu elektronicznego**
Cel: zapewnienie bezpieczeństwa usług handlu elektronicznego oraz ich bezpiecznego używania

– **Monitorowanie**
Cel: wykrywanie nieautoryzowanych działań związanych z przetwarzaniem informacji

7. Kontrola dostępu

– **Wymagania biznesowe wobec kontroli dostępu**
Cel: kontrolowanie dostępu do informacji

– **Zarządzanie dostępem użytkowników**
Cel: zapewnienie dostępu autoryzowanym użytkownikom i zapobieganie nieuprawnionemu dostępowi do systemów informacyjnych

– **Odpowiedzialność użytkowników**
Cel: zapobieganie nieautoryzowanemu dostępowi użytkowników oraz naruszeniu bezpieczeństwa lub kradzieży informacji i środków przetwarzania informacji

– **Kontrola dostępu do sieci**
Cel: ochrona usług sieciowych przed nieautoryzowanym dostępem

– **Kontrola dostępu do systemów operacyjnych**
Cel: ochrona przed nieuprawnionym dostępem do systemów operacyjnych

– **Kontrola dostępu do aplikacji**
Cel: ochrona przed nieautoryzowanym dostępem do informacji przechowywanych w aplikacjach

– **Przetwarzanie mobilne i praca na odległość**
Cel: zapewnienie bezpieczeństwa informacji przy przetwarzaniu mobilnym i pracy na odległość

8. **Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych**
   - **Wymagania bezpieczeństwa systemów informacyjnych**
     Cel: sprawienie, by bezpieczeństwo było integralną częścią systemów informacyjnych
   - **Poprawne przetwarzanie w aplikacjach**
     Cel: ochrona przed błędami, utratą, nieuprawnioną modyfikacją lub nadużyciem informacji w aplikacjach
   - **Zabezpieczenia kryptograficzne**
     Cel: ochrona poufności, autentyczności i integralności informacji poprzez mechanizmy kryptograficzne
   - **Bezpieczeństwo plików systemowych**
     Cel: zapewnienie bezpieczeństwa plików systemowych
   - **Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej**
     Cel: utrzymywanie bezpieczeństwa informacji oraz oprogramowania aplikacyjnego
   - **Zarządzanie podatnościami technicznymi**
     Cel: redukcja ryzyk wynikających z wykorzystania opublikowanych podatności technicznych
9. **Zarządzanie incydentami związanymi z bezpieczeństwem informacji**
   - **Zgłaszanie słabości i zdarzeń związanych z bezpieczeństwem informacji**
     Cel: sprawienie, by zdarzenia związane z bezpieczeństwem informacji oraz słabości związane z systemami informatycznymi były zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących
   - **Zarządzanie incydentami związanymi z bezpieczeństwem informacji i udoskonalenia**
     Cel: sprawienie, by stosowane było spójne i efektywne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji
10. **Zarządzanie ciągłością działania**
    - **Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania**
      Cel: przeciwdziałanie przerwom w działalności biznesowej oraz ochrona krytycznych procesów biznesowych przed rozległymi awariami systemów informacyjnych lub katastrofami, a także zapewnienie wznowienia działalności w wymaganym czasie
11. **Zgodność**
    - **Zgodność z przepisami prawnymi**
      Cel: unikanie naruszania jakichkolwiek przepisów prawa, zobowiązań wynikających z ustaw, regulacji wewnętrznych lub umów oraz jakichkolwiek wymagań bezpieczeństwa
    - **Zgodność z politykami bezpieczeństwa i normami oraz zgodność techniczna**
      Cel: zapewnianie zgodności systemów z normami i politykami bezpieczeństwa organizacji
    - **Rozwiązania dotyczące audytu systemów informacyjnych**
      Cel: maksymalizowanie efektywności procesu audytu systemu informacyjnego i minimalizowanie zakłóceń z niego wynikających lub na niego wpływających

4. Uwagi końcowe

Zarządzanie bezpieczeństwem informacji jest zjawiskiem stosunkowo nowym na rynku polskim, w przeciwieństwie do sytuacji w krajach rozwiniętych, i często niewłaściwie rozpoznanym oraz interpretowanym przez kierownictwo lub personel działów informatycznych organizacji.

Systemy zarządzania bezpieczeństwem są coraz bardziej skomplikowane, a proces ich opracowania jest coraz bardziej kosztowny.

Znaczenia nabiera problem oceny jakości samych systemów, ale także prawidłowości procesu ich opracowania i wdrażania.

Celem artykułu jest wskazanie prawidłowego podejścia do zagadnienia zarządzania bezpieczeństwem informacji poprzez wykorzystanie mniej znanej, ale silnie umocowanej normatywnie metodyki opartej na ISO/IEC 27001.

Ze względu na ograniczony zakres opracowania przedstawiono jedynie podstawowe wytyczne dotyczące wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Jak do tej pory brakuje wyczerpujących opisów dotyczących wdrażania systemów zarządzania bezpieczeństwem informacji. Istniejące modele systemów zarządzania dedykowane są wybranym podsystemom działania lub określonemu obszarowi funkcjonowania organizacji.

Sposoby wdrażania modelowych systemów zarządzania bezpieczeństwem działania nie są jeszcze w pełni ujednolicone (choć istnieje już w tej dziedzinie kilka uznanych standardów, np. omawiany w pracy ISO/IEC 27001).

Porównanie najważniejszych standardów wskazuje na dużą spójność prezentowanych przez różne organizacje podejść do problematyki zarządzania bezpieczeństwem, a także na zgodność zalecanych praktyk i procedur.

Ważnym problemem w SZBI jest prowadzenie audytów systemów informatycznych.

Do chwili obecnej nie ma w pełni ustandaryzowanej metodyki prowadzenia prac i dochodzenia do finalnych ocen audytu – w tym zakresie punktem odniesienia pozostają jedynie dobre praktyki.

Innym z błędów w procesach zarządzania jest skupienie się na obszarze podsystemu IT.

Obserwowany jest także brak elementów optymalizacji kosztów działania w obszarze bezpieczeństwa.

Jednocześnie wzrasta zainteresowanie tym standardem, co zostało zaprezentowane na wykresie 1[2].

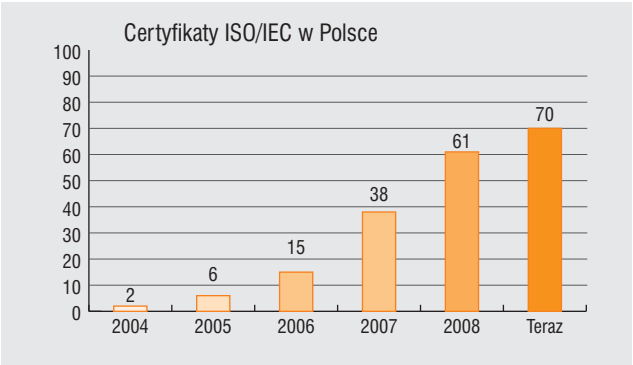
Na wykresie 2 przedstawiono z kolei rozkład uzyskanych certyfikatów wg branż. Z wykresu wynika, że nowe technologie i usługi są branżami wiodącymi w certyfikacji.

Niespodzianką jest wzrost zainteresowania certyfikacją w administracji.

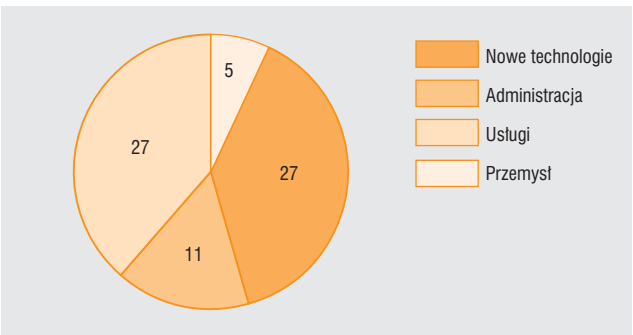
5. Podsumowanie

W artykule przedstawione zostało zastosowanie wytycznych do podsystemu informatycznego organizacji, ale zgodnie z intencją normy nie ma ograniczeń branżowych i można ją stosować we wszystkich organizacjach. System Zarządzania Bezpieczeństwem Informacji, wdrożony zgodnie z ISO/IEC 27001 w dowolnej organizacji, ma charakter uniwersalny. Zawarte w metodyce zasady są otwarte i można je uzu-

2) Na podstawie informacji zawartych w witrynie http://www.iso27000.pl/ firmy PBSG



Wykres 1. Zrealizowane certyfikaty ISO/IEC w Polsce (stan na październik 2008 r.)



Wykres 2. Rozkład uzyskanych certyfikatów wg branż

pełnić o inne specjalistyczne wymagania i zabezpieczenia, adekwatne do prowadzonej przez organizację działalności. Przykładem tego może być uzupełnienie wymagań w zakresie zabezpieczenia przed ulotem elektromagnetycznym urządzeń i systemów teleinformatycznych przetwarzających informacje.

W artykule przedstawiono uznane standardy zarządzania bezpieczeństwem informacji oraz uregulowania prawne i wytyczne branżowe.

Na przykładzie modelu PDCA wskazane zostały zasady wykorzystania właściwych metodyk i standardów do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, obejmujących wszystkie fazy wykorzystywane w procesach SZBI.

Interdyscyplinarny charakter zarządzania bezpieczeństwem informacji wymaga od specjalistów zajmujących się tym zagadnieniem rozległej wiedzy z różnych dziedzin zarządzania, informatyki, prawa, kryminalistyki, inżynierii systemów, psychologii itd. Jednocześnie wszystkie obszary wiedzy nie mogą funkcjonować w oderwaniu od siebie, muszą tworzyć jednolity, synergetyczny System Zarządzania Bezpieczeństwem Informacji. Koordynacją działań powinni zajmować się w organizacji specjalnie do tego powołani menedżerowie ds. bezpieczeństwa.

Należy wyrazić nadzieję, że zakres zagadnień przedstawionych w opracowaniu spotka się z akceptacją i pozwoli przybliżyć szerszemu kręgowi odbiorców problematykę zarządzania bezpieczeństwem informacji w organizacjach, a także pozwoli osobom zainteresowanym kontynuować poznawanie przedstawionych zagadnień w innych ujęciach tematycznych.

Wszyscy zainteresowani zgłębieniem opisanych zagadnień mogą skorzystać ze specjalistycznej literatury i opisów zawartych w Internecie.

Poniżej przedstawiono wybór pozycji i źródła informacji na ten temat.

Literatura:

1. Marian Molski, Małgorzata Łacheta, *Przewodnik audytora systemów informatycznych*, Helion 2007.
2. Andrzej Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WN-T 2006.
3. Ross Anderson, *Inżynieria zabezpieczeń*, WNT 2005.
4. Kevin Lam i inni, *Ocena bezpieczeństwa sieciowego*, Microsoft 2005.
5. Eric Cole i inni, Bezpieczeństwo sieci, Helion 2005.
6. Krzysztof Czerwiński, *Audyt wewnętrzny*, InfoAudit 2005.
7. Edward Yourdon, *Wojny na bity*, WNT 2004.
8. Krzysztof Liderman, *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Mikom 2003.
9. Krzysztof Liderman, *Bezpieczeństwo teleinformatyczne*, WSISiZ 2003.
10. Marian Molski, Sebastian Opala, *Elementarz bezpieczeństwa systemów informatycznych*, Mikom 2002.
11. Donald L. Pipkin, *Bezpieczeństwo informacji*, WNT 2002.
12. Dorothy E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, WNT 2002.
13. Eric Maiwald, *Bezpieczeństwo w sieci. Kurs podstawowy*, 2000, 2001.
14. Tadeusz Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Helion 1999.

Normy i standardy:

1. PN ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji. Wymagania.
2. PN ISO/IEC 17799:2005 Praktyczne zasady zarządzania bezpieczeństwem informacji.
3. PN ISO/IEC 15408-1:2001 Kryteria oceny zabezpieczenia systemów. Model ogólny oceny zabezpieczenia systemów.
4. PN ISO/IEC 15408-3:2002 Kryteria oceny zabezpieczenia systemów. Wymagania uzasadnienia pewności.
5. PN ISO/IEC 17799:2003 Praktyczne zasady zarządzania bezpieczeństwem informacji.
6. PN-I-13335-1:1998 Wytyczne do zarządzania bezpieczeństwem systemów informacyjnych – Pojęcia i modele bezpieczeństwa systemów informatycznych.

Strony internetowe:

– http://www.iso27000.pl/
– http://www.bsigroup.pl/
– http://www.tuv-nord.pl/

Referaty:

– Prezentacja – Janusz Cendrowski, Krajowa Konferencja Zastosowań Kryptografii Enigma, 2005 r.
– Prezentacja – Marek Blim, *Ochrona informacji*, 2006 r.
– Prezentacja – Andrzej Wójcik, *Polityka bezpieczeństwa. Wybrane zagadnienia*, 2006 r.

DR INŻ. ANDRZEJ WÓJCIK

artykuł sponsorowany

Harmony

Zintegrowany system zarządzania personelem

Zintegrowany system zarządzania personelem w przedsiębiorstwie umożliwia zwiększenie wydajności pracy, a także skuteczną kontrolę nad bezpieczeństwem danych i mieniem firmy. Najnowocześniejsze systemy oferują nieograniczone możliwości rozbudowy struktury systemu i jego elastycznego dopasowywania do potrzeb konkretnej instytucji. Jak zatem można zintegrować i zautomatyzować poszczególne procesy związane z zarządzaniem, biorąc pod uwagę problemy wynikające z konieczności wdrażania kilku aplikacji i rozdzielnych systemów? Warto rozważyć skorzystanie z rozwiązania oferowanego przez firmę Control System FMN – systemu Harmony stworzonego przez firmę Synel Industries

Harmony to rozwiązanie programowe, wspierające procesy zarządzania przedsiębiorstwem w zakresie kontroli personelu i gości oraz zapewnienia bezpieczeństwa. Program wspomaga zarządzanie zasobami firmy przy wykorzystaniu systemów kontroli dostępu, rejestracji czasu pracy, telewizji dozorowej, kontroli przeciwpożarowej i systemów alarmowych. Integruje i systematyzuje procesy administrowania firmą, optymalizuje wykorzystanie zasobów ludzkich oraz koszty ich eksploatacji.

Platforma Harmony jest pakietem modułów wspomagających zarządzanie przedsiębiorstwem. Jej podstawowe funkcje obejmują system kontroli dostępu i ewidencji czasu pracy pracowników. System pozwala na zarządzanie informacjami o personelu, w tym na kontrolę ruchu personelu, monitoring obecności, kontrolę dostępu – wszystko, co jest w tym celu potrzebne, jest zawarte w jednym programie. Współpracujące ze sobą moduły platformy Harmony **eliminują potrzebę prowadzenia niezależnych baz danych**. Zewnętrzny moduł raportowania w sieci zwiększa bezpieczeństwo firmy.

Modułowa struktura programu pozwala na wykorzystywanie tylko tych funkcji, które są potrzebne, bez konieczności kupowania i instalowania wszystkich modułów, co pozwala optymalizować koszty systemu w zależności od jego funkcjonalności.

Moduł rozliczania czasu pracy daje szerokie możliwości dokładnego i efektywnego rozliczania pracownika w celach płacowych. System gromadzi wszystkie dane obecności, uwzględniając zasady pracy, a następnie przelicza w czasie rzeczywistym przepracowane godziny, tworząc raporty do kalkulacji płac. Poniżej wyszczególniono główne zalety rozwiązania:

- system wielozadaniowy,
- system pracujący *on-line*, umożliwiający podgląd w czasie rzeczywistym obecności/ nieobecności pracownika,
- elastyczne parametry i zasady pracy,
- wiele formatów kalendarza,
- pięć stref bezpieczeństwa: strefa, oddział, sekcja, wydział, stanowisko pracy, które są dostosowywane w zależności od potrzeb klienta,
- dynamiczna autoryzacja systemu raportowania, okien i menu, autoryzacja odczytu lub odczytu/zapisu w tabelach,
- zmienne raporty, opcja generowania nowych raportów lub edytowanie istniejących,
- elastyczne opcje eksportu i importu plików,
- raporty graficzne dla menadżerów,
- format raportów (XLS lub PDF), opcja wysyłania raportów przez e-mail.

Moduł kontroli dostępu zawiera interfejs telewizji dozorowej, zapewnia drukowanie spersonalizowanych kart i synchronizowanie map aktywnych. Moduł jest potężnym narzędziem, pozwalającym na kontrolowanie zarówno pracowników, jak i miejsca pracy.

Pozwala na limitowanie dostępu do określonych stref, podgląd w czasie rzeczywistym dokładnego położenia każdego pracownika, generuje raporty lokalizacji i ruchu wszystkich osób w celach ochrony i bezpieczeństwa. Cechy i elementy charakterystyczne modułu to:

– autoryzacja wejścia w zależności od stref/przedziałów czasowych/statusu pracownika,
– interfejs internetowy (WEB) gości,
– alarm w przypadku próby sforsowania drzwi lub drzwi otwartych,
– raport dotyczący obecności oraz raport gości,
– połączenie z systemem kontroli obecności (pierwsze zalogowanie – wejście, ostatnie – wyjście),
– opcja graficznego przedstawiania zdarzeń,
– podgląd strefowy zdarzeń *on-line*,
– powiadomienie alarmowe przez SMS, e-mail, wyskakujące okno (*pop-up*),
– tworzenie procedur reagowania na zdarzenia alarmowe,
– podział zdarzeń ze względu na ważność i priorytet.

Moduł kosztów pracy – procedury i metody pracy mogą stać się efektywniej wyznaczane na podstawie gromadzonych z danego działu danych. Dane te stanowią podstawę do podejmowania właściwych decyzji. Moduł kosztów pracy pozwala kontrolować i poprawnie wyznaczać czas przeznaczony na różne zadania, a także wyliczyć koszty wiążące się z realizacją poszczególnych projektów. Jest to wyjątkowo efektywne narzędzie, pozwalające zarządzać kosztami projektów w firmie.

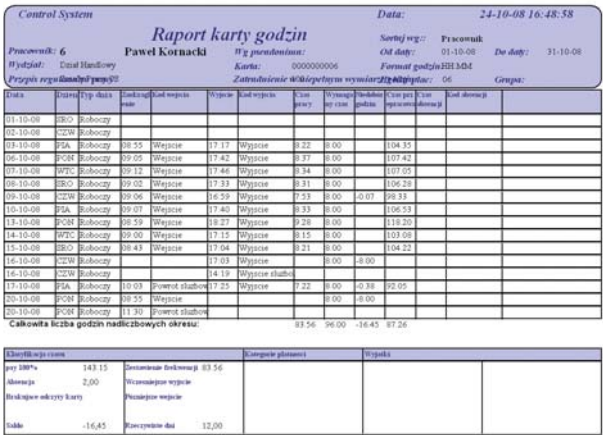
Moduł interfejsu WEB użytkownika umożliwia współpracę z siecią Intranet organizacji i zapewnia dostęp do systemu wszystkim użytkownikom. Dostęp do danych jest przydzielany na innym poziomie, w zależności od pozycji każdego pracownika i poziomu autoryzacji. Pracownik może przeglądać i aktualizować swój raport czasowy, podczas gdy menedżer może przeglądać i zatwierdzać dane pracownika na określonych poziomach. Moduł zapewnia:

– możliwość raportowania obecności/zleceń każdego stanowiska w czasie rzeczywistym,
– aktualizację zmian tylko po zaakceptowaniu przez menedżera,
– możliwość generowania raportów w zależności od poziomu autoryzacji (menedżer/pracownik),
– możliwość korekcji danych przez użytkownika za zgodą menedżera,
– definiowanie nowych pracowników oraz aktualizację danych pracowników obecnych,
– opcję produkcji dodatkowego identyfikatora dla użytkownika na wypadek utraty poprzedniego,
– różnorodne raporty, które mogą być generowane według rożnych specyfikacji i zapisywane w formacie DOC, XLS lub PDF w wersji tylko do odczytu lub druku.

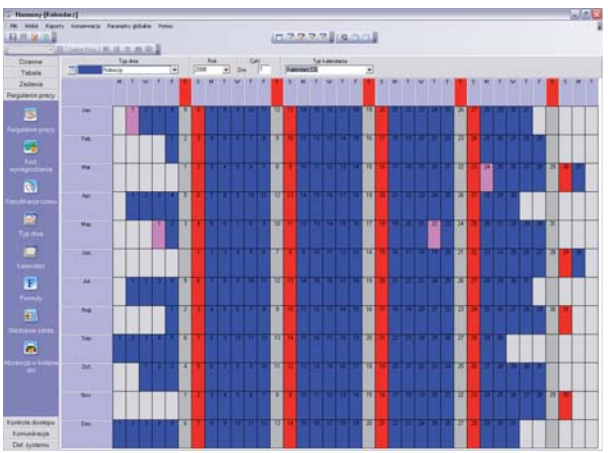
Harmony jest nowoczesną platformą umożliwiającą sprawne zarządzanie zasobami ludzkimi i bezpieczeństwem w dużych i średnich przedsiębiorstwach. Jej niewątpliwą zaletą jest działanie wszystkich modułów na jednej bazie danych i możliwość integracji z innymi programami działającymi w firmie, takimi jak oprogramowanie HR czy programy płacowe. Ważnym atutem jest również fakt, że firma Synel Industries jest jednocześnie producentem takich urządzeń, jak czytniki i zegary czasu pracy, które wraz z oprogramowaniem tworzą jednolity i niezawodny system.

Więcej informacji na temat działania systemu można uzyskać u wyłącznego dystrybutora opisywanych urządzeń i oprogramowania – firmy Control System FMN (tel. 022 8550017, www.cs.pl).

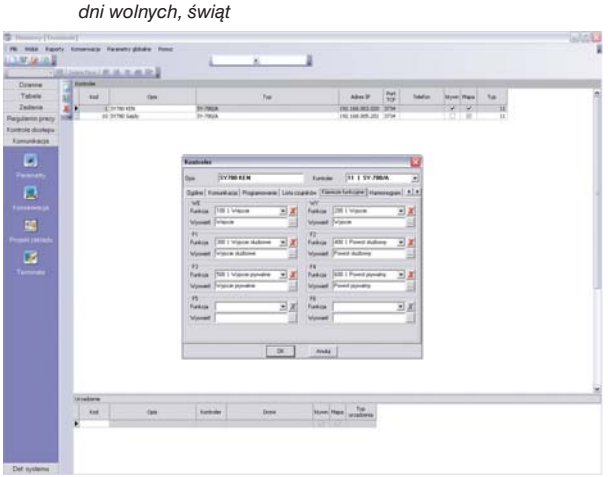
CONTROL SYSTEM FMN



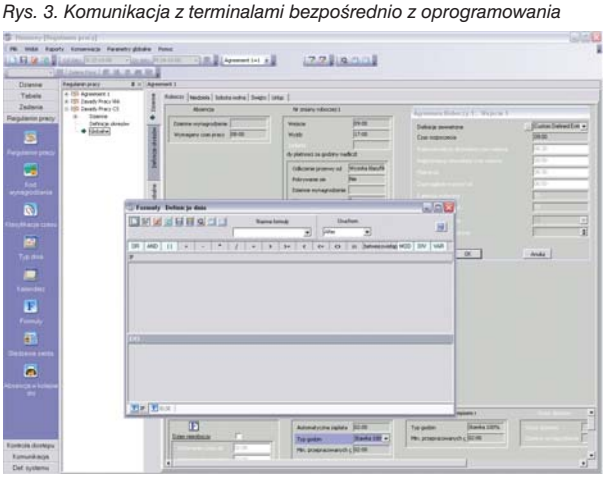
Rys. 1 Przejrzyste raporty – gotowe szablony oraz możliwość tworzenia własnych wzorów



Rys. 2. Kalendarz umożliwiający sprawne wprowadzanie dni roboczych, dni wolnych, świąt



Rys. 3. Komunikacja z terminalami bezpośrednio z oprogramowania



Rys. 4. Możliwość ustawiania zaawansowanych zasad pracy zatrudnionych pracowników

Kioski bankowe

Gunnebo Polska

Co zyskujemy dzięki kioskom bankowym Gunnebo Polska? Lepszą dostępność dla klienta, mniejsze koszty dla banku, zwiększone bezpieczeństwo obsługi

Kioski bankowe to małe wolnostojące „placówki bankowe", dostępne dla klientów przez 24 godziny na dobę przez siedem dni w tygodniu.

Zapewniają one efektywną pod względem kosztów alternatywę względem tradycyjnych oddziałów banku, a ponadto umożliwiają dostarczenie usług bankowych w odległych miejscach.

Kioski mogą być wykonane na różnych poziomach zabezpieczenia (panele o różnych klasach odporności włamaniowej), w zależności od lokalizacji oraz rodzaju urządzeń samoobsługowych, które mają być w kiosku zainstalowane.

Kioski bankowe mogą być montowane zarówno na zewnątrz budynków, np. na parkingach lub obok stacji paliw, jak i wewnątrz galerii handlowych. Firmy transportujące gotówkę oraz serwisujący technicy mają dostęp do kiosku przez zewnętrzne drzwi skarbcowe i/lub odpowiednio zaaranżowany system śluzowy.

Standardowe kształty kiosków to bryły o podstawie prostokąta i ośmiokąta. Dzięki modułowej budowie dostępne są jednak również inne kształty kiosków. Możliwe jest także dostosowanie ich do lokalnych wymagań banku.

Bogusław Szkudlarek
Szymon Biernacki
Gunnebo Polska

Podsystemy diagnostyczne

w systemach sygnalizacji włamania i napadu (część 1)

Podczas eksploatacji systemów sygnalizacji włamania i napadu (SSWiN) występują różnego rodzaju czynniki zewnętrzne, które powodują, że każdy z systemów po pewnym czasie od chwili uruchomienia znajduje się w innym stanie technicznym. Wynika z tego konieczność podejmowania określonych decyzji eksploatacyjnych w odniesieniu do tych systemów. Ułatwienie zarządzania procesem eksploatacyjnym wymusiło na producentach urządzeń wyposażanie ich w coraz bardziej zaawansowane podsystemy diagnostyczne, umożliwiające określenie stanu technicznego i podjęcie racjonalnych działań w celu zwiększenia gotowości realizacji zadań przez te systemy. Niniejszy artykuł przedstawia ewolucję podsystemów diagnostycznych stosowanych w SSWiN. W cz. 1 omówione zostaną związane z nimi postanowienia normy PN-EN-50131-1:2007 oraz geneza podsystemów diagnostycznych, natomiast w cz. 2 zaawansowane podsystemy diagnostyczne, stosowane głównie w SSWiN o strukturze rozproszonej

Wymagania stawiane podsystemom diagnostycznym

Chociaż stosowanie norm nie jest obowiązkowe, prawie wszystkie firmy produkujące urządzenia SSWiN uwzględniają już na etapie projektowania wbudowane podsystemy diagnostyczne. Zwiększa to koszt produkcji, ale dzięki temu możliwe jest spełnienie wymagań zawartych w odpowiednich normach. Jednocześnie projektant, instalator, użytkownik i konserwator SSWiN dostają system, który ma możliwość określenia uszkodzenia poszczególnych jego podsystemów lub elementów.

Norma europejska EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", która ma jednocześnie status Polskiej Normy PN-EN 50131-1:2007 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe", zawiera wskazania dotyczące uszkodzeń systemu. Podaje ona definicje i skróty, m.in.:

- stan uszkodzenia: stan systemu alarmowego uniemożliwiający normalne działanie systemu alarmowego sygnalizacji włamania lub jego części,
- sygnał/komunikat uszkodzenia: informacja wytwarzana wskutek uszkodzenia.

Przytoczone definicje są niezwykle istotne, gdyż jeśli np. wystąpi stan uszkodzenia, to oznacza to, iż SSWiN nie w pełnym zakresie spełnia stawiane mu wymagania dotyczące zapewnienia ochrony osób i mienia. Taki stan jest niedopuszczalny z punktu widzenia użytkownika systemu, ale nie jest możliwe całkowite wyeliminowanie go spośród stanów eksploatacyjnych, które mogą wystąpić w rzeczywistych warunkach pracy. Jednak dzięki informacjom pochodzącym z podsystemów diagnostycznych możliwe jest szybkie zareagowanie na powstałą sytuację i podjęcie odpowiednich działań zmierzających do usunięcia awarii i jednocześnie przywrócenia stanu zdatności systemu, serwisant ma ułatwione zadanie w poszukiwaniu miejsca uszkodzenia, a jednocześnie uzyskuje w pewnym stopniu (zależnie od zastosowanego podsystemu diagnostycznego) wiedzę dotyczącą rodzaju i wielkości uszkodzenia.

Systemy alarmowe sygnalizacji włamania zawierają najczęściej następujące części składowe:

- centralę alarmową,
- jedną lub więcej czujek,
- jeden lub więcej sygnalizatorów i (lub) systemów transmisji alarmu,
- jeden lub więcej zasilaczy.

Nie jest wymieniony podsystem diagnostyczny. Jednak norma PN-EN 50131-1:2007, w rozdziale dotyczącym funkcjonowania, podaje stwierdzenie, że system alarmowy sygnalizacji włamania powinien zawierać środki umożliwiające wykrycie włamywacza, sabotażu i rozpoznanie uszkodzeń. Oznacza to, że bez możliwości zastosowania podsystemu diagnostycznego nie jest możliwe spełnienie wymagań zawartych w normie. W rzeczywistości nie jest tak do końca, ponieważ przy całkowitej integracji podsystemów w jeden system trudno jest czasem wyróżnić wyraźnie podsystem diagnostyczny. Zazwyczaj jego zadania przejmuje wtedy system zintegrowany, który odpowiada także za wiele innych czynności, np. ustawianie parametrów funkcjonalnych, korektę wpływu zakłóceń elektromagnetycznych itp.

Norma PN-EN-50131-1:2007 wymienia również uszkodzenia, które mają być wykrywane i jednocześnie ma być zapewniona możliwość ich zobrazowania. Należą do nich m.in.:

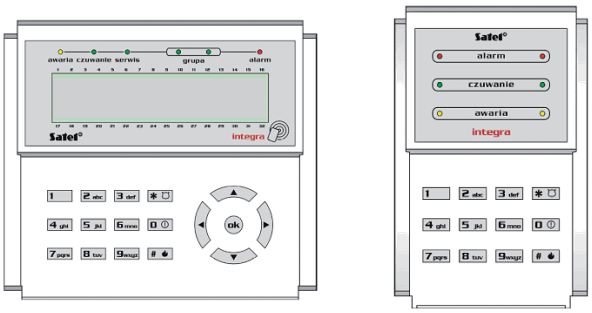
- uszkodzenie zasilacza podstawowego,
- uszkodzenia zasilacza rezerwowego,
- uszkodzenie łączności (transmisji komunikatów i/lub sygnałów między elementami składowymi systemu alarmowego),
- uszkodzenie systemu (lub systemów) transmisji alarmu (jeśli jest zastosowany w SSWiN),
- uszkodzenie sygnalizatora (sygnalizatorów).

Dopuszcza się, by inne rodzaje uszkodzeń były rozpoznawane i obrazowane, pod warunkiem, że nie wpływa to niekorzystnie na rozpoznawanie uszkodzeń wymienionych powyżej. Zazwyczaj podsystemy diagnostyczne mają tak duże możliwości, że nie ograniczają się tylko do wykrywania wymienionych czterech rodzajów niesprawności (co jest bardzo korzystne z punktu widzenia konserwatora systemu).

W przypadku wystąpienia uszkodzenia jest wymagane przesłanie informacji o tym fakcie do alarmowego centrum odbiorczego przez system transmisji alarmu. Gdy system sygnalizacji włamania jest w stanie włączenia, dla klasy zabezpieczenia 1 dopuszcza się rodzaj komunikatu: „Alarm" lub „Uszkodzenie", zaś dla klasy 2, 3 i 4 musi być to zdefiniowane jednoznacznie, czyli: „Uszkodzenie". Gdy system sygnalizacji włamania jest w stanie wyłączenia, dla klasy zabezpieczenia 1 i 2 dopuszcza się zastosowanie opcjonalnie komunikatu: „Uszkodzenie", zaś dla klasy 3 i 4 komunikat „Uszkodzenie" jest obowiązujący.

Geneza podsystemów diagnostycznych

Wymienione w poprzednim rozdziale artykułu zalecenia są zawarte w polskiej normie PN-EN-50131-1. Zanim jednak zostały one tam uwzględnione, już wiele lat wcześniej zajmowano się diagnostyką. Termin ten pochodzi od greckiego słowa diagnosis – czyli rozpoznanie. Słowo to kojarzone było początkowo w starożytności z medycyną, która zajmowała się rozpoznawaniem



Rys. 1. Przykład prostego zobrazowania wystąpienia uszkodzenia w SSWiN: z lewej manipulator typu LCD, z prawej manipulator strefowy typu LED

Fot. 1. Zobrazowanie uszkodzenia zasilania podstawowego i rezerwowego z wykorzystaniem diod LED

chorób na podstawie objawów występujących u chorej osoby. Z upływem lat termin ten rozszerzono, obejmując nim także przedmioty materialne, m.in. urządzenia i systemy. Nadal jednak chodzi o sformułowanie oceny, w jakim stanie znajduje się badany obiekt, na podstawie cech tego stanu – np. wielkości fizycznych lub ekonomicznych (takich jak nakłady finansowe związane z konserwacją SSWiN, zwiększone koszty energii elektrycznej przy doładowywaniu wyeksploatowanego akumulatora itp.), które charakteryzują stan obiektu podczas eksploatacji. W tym celu podczas etapu projektowania systemów zakłada się konieczność zastosowania podsystemów diagnostycznych. Koncepcja ich działania powinna uwzględniać to, jaki charakter będzie miała ich praca:

- automatyczny czy nieautomatyczny,
- czy będą mierzone wartości ciągłe czy dyskretne (a może oba rodzaje),
- jak będzie dokonywana akwizycja mierzonych wartości,
- jaką strukturę niezawodnościową będzie miał podsystem diagnostyczny i jaki układ samokontroli będzie zastosowany,
- czy będzie zastosowany układ decyzyjny ułatwiający wnioskowanie diagnostyczne,
- jak będą prezentowane wyniki pomiarów.

Można tak zaprojektować podsystem diagnostyczny, aby realizował wiele więcej funkcji niż te, które wymieniono. Jednak wszystko zależy od kosztów takiego rozwiązania. Zaletą podsystemów rozbudowanych jest to, iż znacznie obniżają one koszty eksploatacji poprzez:

- zmniejszenie kosztów związanych z diagnostyką systemów (np. możliwe jest zdalne wykonanie tej czynności poprzez wykorzystanie sieci WAN[1], LAN[2], GSM[3] czy telefonicznej),
- zmniejszenie czasów przeglądów okresowych dzięki zautomatyzowaniu procesu diagnostycznego,
- zwiększenie liczby informacji diagnostycznych, a tym samym zwiększenie zakresu badań diagnostycznych i wiarygodności postawionych hipotez,
- zmniejszenie liczby personelu diagnostycznego (jeśli zastosowano zdalną diagnostykę),
- otrzymanie informacji o rodzaju uszkodzenia, a tym samym szybsze znalezienie miejsca awarii (szczególnie istotne w przypadku SSWiN o strukturze rozproszonej).

Jak wynika z powyższych rozważań, z jednej strony należy dążyć do stosowania bardzo rozbudowanych i złożonych algorytmicznie podsystemów diagnostycznych, z drugiej zaś koszty takich rozwiązań są znaczne i nierzadko przekraczają koszt samego systemu. Wszystko zależy od tego, gdzie SSWiN ma być zastosowany i jakie dobra materialne i niematerialne będzie chronił (np. materiały radioaktywne, związki chemiczne groźne dla środowiska).

Niezależnie od stopnia złożoności podsystemu diagnostycznego, zazwyczaj najsłabszym punktem jest człowiek (zwłaszcza użytkownik systemu) i to on jest odpowiedzialny za niepodjęcie odpowiednich działań. Wynika to najczęściej z faktu, iż źle przeszkolony lub w ogóle nieprzeszkolony użytkownik SSWiN nie wie, co mu system „pokazuje". Dlatego też producenci najczęściej ograniczają się do zobrazowania informacji o wystąpieniu uszkodzenia na przeznaczonym do tego celu elemencie systemu (np. przez umieszczenie diody LED oznaczonej „AWARIA" na klawiaturze – rys. 1 – lub na tablicy synoptycznej) albo na ekranie monitora przy zastosowaniu nadzoru komputerowego. Użytkownik powinien wtedy, przy wykorzystaniu wiedzy zdobytej podczas szkolenia w czasie przekazywania mu systemu, wykonać odpowiednie czynności przewidziane przez producenta i określić rodzaj uszkodzenia, a następnie wezwać serwis w celu usunięcia awarii.

Jeśli SSWiN jest monitorowany, to powinno się przekazać informację o uszkodzeniu i jego rodzaju do alarmowego centrum odbiorczego. Podejmie wtedy ono odpowiednie działania zmierzające do naprawy awarii. Zazwyczaj w przypadku małych obiektów (jakimi są np. domki jednorodzinne) firmy świadczące usługi monitorowania wykorzystują następujące informacje:

- brak zasilania sieciowego 230 V,
- awaria akumulatora (za niskie napięcie).

W niektórych typach SSWiN informacje te są zobrazowane osobnymi diodami LED[4] (fot. 1).

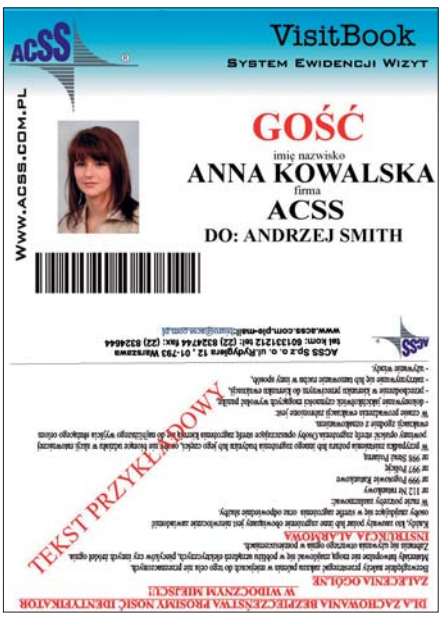
DR INŻ. ADAM ROSIŃSKI

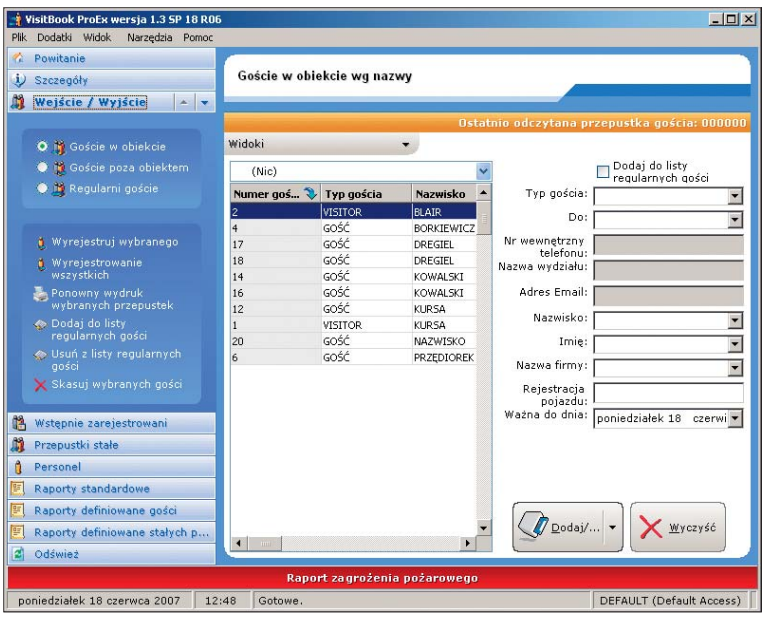
Literatura:

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

1) WAN – rozległa sieć komputerowa, ang. *Wide Area Network*
2) LAN – lokalna sieć komputerowa, ang. *Local Area Network*
3) GSM – system mobilnej telefonii komórkowej, ang. *Global System for Mobile Communications*
4) LED – dioda elektroluminescencyjna, ang. *Light Emitting Diode*

System rejestracji gości VisitBook





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

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

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

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

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

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

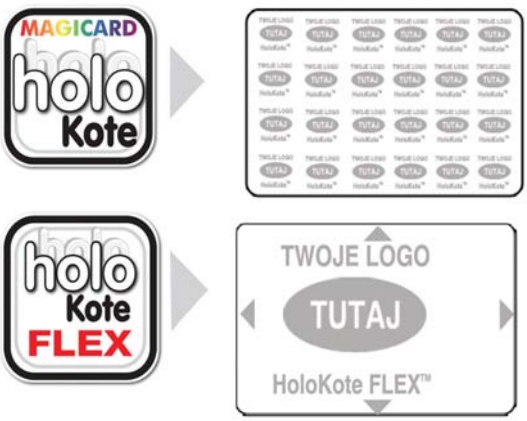
Wydruk przepustek jest możliwy na standardowych drukarkach biurowych oraz drukarkach do kart PVC (tylko wersja Pro-Ex i xFR). Główną zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym, np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program ponadto zawiera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

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

Profesjonalne drukarki do kart PVC

MAGICARD

Kolorowe drukarki do kart identyfikacyjnych PVC z możliwością drukowania znaku wodnego



HoloKote™ - znak wodny drukowany na całej powierzchni karty (24 identyczne grafiki). Widoczny przy patrzeniu pod kątem.

HoloKote FLEX™ - znak wodny drukowany w dowolny rozmiarze i wybranym mejscu na powierzchni karty.

Nadruk od krawędzi do krawędzi z jakością 300 dpi.

HoloPatch™ - okno w rogu karty, w którym znak wodny jest bezpośrednio widoczny (opcja karty).

Dwustronny nadruk - tylko drukarka Tango 2e.

Interfejs Ethernet.

3 lata gwarancji (łącznie z głowicą).

Dodatkowe opcje:

Dowolne tekst lub grafika w znaku wodnym (dotyczy HoloKote™ i HoloKote FLEX™).

Możliwość kodowania kart chipowych i zbliżeniowych.

Możliwość kodowania pasków magnetycznych(opcja).

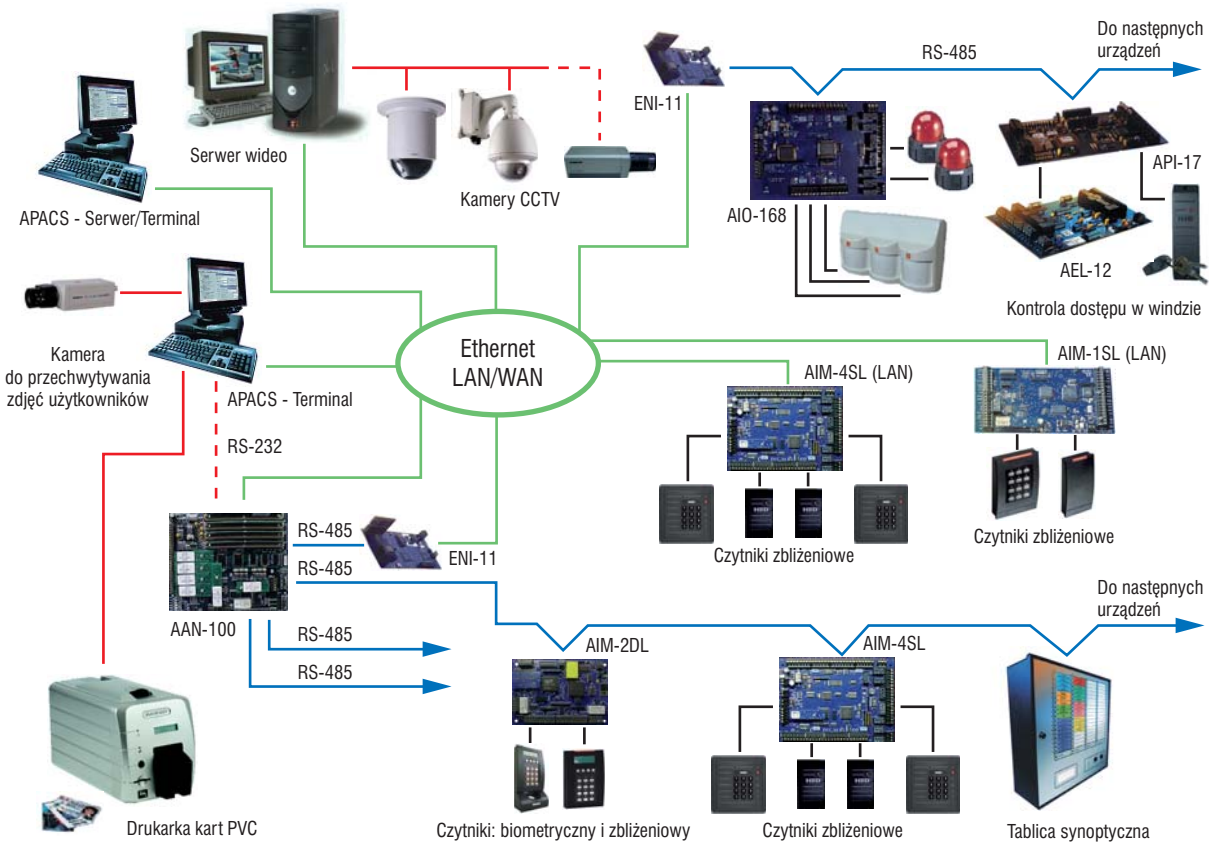
Specyfikacja techniczna
Prędkość nadruku
– Wydruk karty w kolorze w 22 sekundy/stronę – Wydruk karty monochromatycznej w 6 sekund/stronę
Wbudowane zabezpieczenia
– HoloKote™ - znak wodny na całej powierzchni karty (2 wzory) – HoloKote FLEX™- znak wodny drukowany w większym rozmiarze, w dowolnym miejscu na powierzchni karty
Typy taśm
– LC1 : YMCKO 350 wydruków – LC3 : Monochromatyczna 1000 wydruków – LC6 : KO (czarny i overlay) 600 wydruków – LC8 : YMCKOK 300 wydruków (tylko Tango2)
Typy kart
– PVC ISO CR80 z paskiem magnetycznym, zbliżeniowe, samoprzylepne oraz karty z HoloPatch™
Grubość kart
– 0,38 mm do 1,6 mm
Pojemność magazynków
– Podajnik 100 szt. – Odbiornik kart nadrukowanych 50 szt.
Głowica
– 300 dpi
Interfejs
– Port USB, Ethernet
Sterowniki
– Sterowniki w języku polskim pod Windows 2000, XP, Vista
Zasilanie
– 90-265V 47-63 Hz
Wymiary
– Rio 2e – 193,5 (szer.) x 232,5 (wys.) x 369,5 (dł.) mm – Tango 2e – 193,5 (szer.) x 232,5 (wys.) x 471,1 (dł.) mm
Waga
– Rio 2e – 7,2 kg – Tango 2e – 8,3 kg
Temperatura pracy
– od 10°C do 30°C

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa

tel. (22) 832 47 44, faks (22) 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl, http://www.magicard.com.pl

Zintegrowany system zabezpieczeń firmy Apollo

APOLLO wraz z oprogramowaniem APACS stanowi kompleksowy system zabezpieczeń obiektu. Integruje: system kontroli dostępu, system sygnalizacji włamania i napadu, telewizję dozorową, kontrolę pracy strażników, moduł obsługi gości. Umożliwia projektowanie i wydruk identyfikatorów pracowniczych oraz realizuje podstawowe funkcje zliczania czasu pracy. Wykorzystując moduły kontroli wind AEL-12, można prowadzić kontrolę dostępu do określonych pięter budynku przy użyciu windy. Użycie modułów wejść/wyjść serii AIO umożliwia sterowanie pracą klimatyzacji bądź oświetleniem. APOLLO jest systemem modułowym dzięki czemu możliwa jest, w dowolnym momencie, jego szybka rozbudowa o kolejne urządzenia. Wszystkie urządzenia mają wymienne interfejsy komunikacyjne, dzięki czemu komunikacja w systemie może odbywać się za pośrednictwem magistrali RS-485 lub sieci lokalnej LAN.

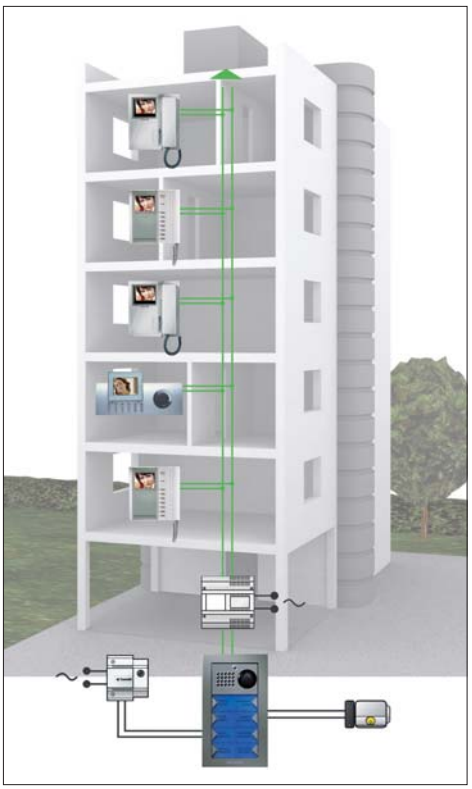


- 32 stacje robocze
- 32 kontrolery główne (AAN)
- 3072 czytniki
- 16 384 linie alarmowe
- 8192 wyjścia przekaźnikowe
- 79 000 zdarzeń off-line (w standardzie)
- 100 dni świątecznych
- 127 stref czasowych (6 przedziałów w każdej strefie)
- 256 poziomów dostępu
- Równoległa obsługa do 8 formatów kart
- Antipassback strefowy (globalny) i czasowy
- Parametryzacja wejść (alarm i kontrola dostępu)
- Wersje Lite, Standard i Professional oprogramowania APACS
- Zaawansowane mechanizmy reakcji systemowych
- Kontrola dostępu w windzie
- Weryfikacja wizyjna
- Graficzne mapy obiektu
- Generowanie raportów wg dowolnego klucza
- Dowolna liczba operatorów systemu z precyzyjne definiowalnymi uprawnieniami
- Funkcja zliczania osób w strefie
- Tablica synoptyczna do wizualizacji stanu systemu
- Autonomiczna praca urządzeń w sytuacji braku komunikacji (moduły z lokalną pamięcią)
- Programowe powiązanie zdarzeń i reakcji pomiędzy systemami SSWiN, KD i CCTV
- 2 kontrolery główne (AAN-32 i AAN-100)
- 4 moduły kontroli czytników (AIM-1/2/4SL i AIM-2DL)
- 3 panele alarmowe (AIO – 8/16/168)
- Pamięć typu flash wszystkich urządzeń systemu

Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa

tel. (22) 663 40 85, faks (22) 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

2-przewodowy, kolorowy system wideodomofonowy firmy COMELIT



SBC SIMPLEBUS COLOR

Cechy systemu:

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

Monitory wewnętrzne dostępne w systemie Simplebus Color

GENIUS

BRAVO

DIVA

PLANUX

Panele wejściowe

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

alarmnet®

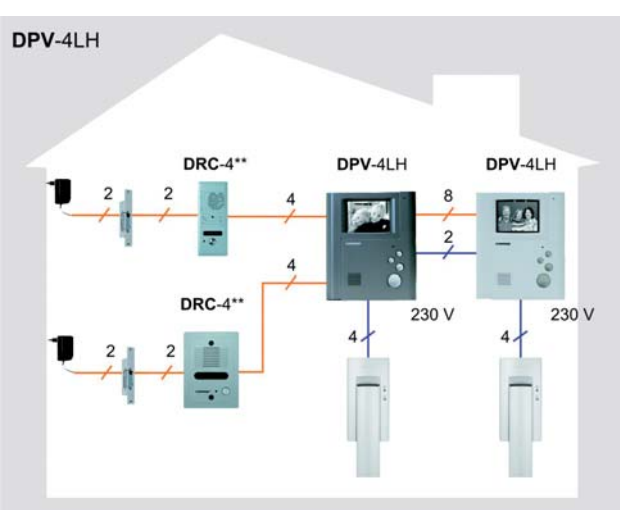
Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa

tel. (22) 663 40 85, faks (22) 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

Monitor DPV-4LH

System wideodomofonowy COMMAX zbudowany w oparciu o monitor DPV-4LH jest ciekawą alternatywą dla prostych domofonów umożliwiających tylko łączność głosową z wejściem. Monitor DPV-4LH pozwala na rozmowę z osobą przy wejściu bez potrzeby podnoszenia słuchawki (system głośnomówiący) oraz umożliwia kontakt wzrokowy wyświetlając obraz z kamery wbudowanej w panel rozmówny lub dowolnej kamery podłączonej do wejścia wideo tego monitora. Monitor ma możliwość obsługi dwóch wejść (poprzez rozbudowę o dodatkowy panel rozmówny), podłączenia dodatkowych monitorów i unifonów (realizacja funkcji interkomu).

Specyfikacja techniczna	
Zasilanie	AC 100 ÷ 240 V; 50 / 60 Hz
Zasilanie	17 V DC
Pobór mocy	maks. 16 W
Ekran monitora	czarno-biały – 4” płaski
Czas wyświetlania obrazu	60 s ±10 %
Okablowanie	28m (ø 0,5) / 50m (ø 0,65) / 70m (ø 0,8)
Temperatura pracy	0°C do + 40°C
Masa	1,2 kg
Wymiary	190 x 226 x 48 mm (szer. / wys. / gł.)



Schemat połączenia DPV-4LH

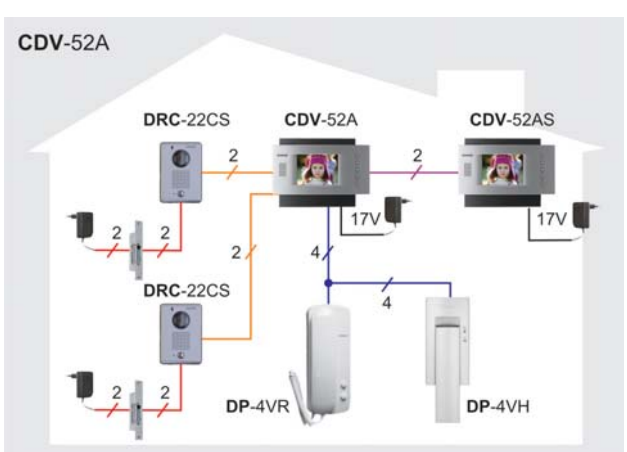
GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne
tel./faks (12) 256 50 35, 256 50 25
faks (12) 270 56 96
e-mail: biuro@gde.pl

Wideodomofon CDV-52A / DRC-22CS

Firma GDE Polska wprowadza na rynek nowy monitor kolorowy dla domów jednorodzinnych pracujących na instalacji 2 żyłowej (połączenie kamera-monitor). Funkcjonalnie jest to odmiana monitora CDV-50A, posiadająca wszystkie jego cechy, czyli możliwość podłączenia drugiej kamery, dodatkowych monitorów (CDV-52AS), czy unifonów (DP-4VH lub DP-4VR). Monitor posiada wysokiej jakości 5-calowy ekran LCD na którym może być wyświetlany obraz z kamery DRC-22CS. Rozmowa z odwiedzającym realizowana jest w sposób głośnomówiący, co eliminuje konieczność podnoszenia słuchawki. Dodatkową funkcją jest możliwość nawiązania połączenia interkomowego wewnątrz budynku (przy podłączonych kilku monitorach lub unifonach).

- monitor kolorowy
- wyświetlacz 5" Color TFT-LCD
- obsługuje dwa wejścia
- możliwość podłączenia dodatkowych monitorów CDV-52AS
- funkcja interkomu
- współpracuje z kamerami DRC-22CS
- zasilanie 17 V DC

Specyfikacja techniczna monitora	
Okablowanie	Monitor - kamera: 2 przewody Monitor - unifon: 4 przewody
Zasilanie	17 V DC
Pobór prądu	Praca: 23 W, czuwanie: 5,5 W
Temperatura pracy	0 - 40°C
Wymiary (szer. / wys. / gł.):	245 mm x 175 mm x 45 mm
Masa:	0,8 kg



GDE POLSKA
Global Distributor of Electronics

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

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

Rejestrator Falcon DF0450LV

Rejestrator Falcon DF0450LV to najmniejszych rozmiarów rejestrator w ofercie Factor Security. Ma on możliwość nagrywania 4 kamer z prędkością 50 kl/s w kompresji Modified MJPEG. Rejestrator pracuje w trybie triplex pozwalając na równoczesne: nagrywanie, odtwarzanie i podgląd przez sieć LAN. Dostęp do ustawień menu zabezpieczony jest hasłem. Rejestrator posiada funkcję nagrywania detekcji ruchu. Oprócz standardowego wyjścia monitorowego typu BNC posiada także dodatkowe wyjście VGA o regulowanej rozdzielczości do podłączenia monitora komputerowego. Do rejestracji obrazu z podłączonych kamer urządzenie używa dysku twardego SATA o pojemności do 1TB. Do wbudowanego portu USB możemy podłączyć pendrive zarówno w celu archiwizacji materiału jak i aktualizacji firmware'u. Rejestrator posiada możliwość podglądu poprzez sieć LAN gdzie wysyła obrazy w kompresji MPEG4.

Specyfikacja techniczna			
Format Wideo	NTSC/PAL		
System	RTOS		
Wyjścia VGA	D-SUB 15Pin VGA		
Wejścia Wideo	BNC x 4 (1Vp-p 75Ω)		
Wejścia Audio	RCA x 1, Line-In		
Wyjścia Wideo	BNC x 1(Monitor główny)		
Wyjście Audio	RCA x 1		
Język menu	wielojęzyczne		
Wyświetlanie		120 kl./s (4 × 30 kl./s)	
	PAL	100 kl./s (4 × 25 kl./s)	
Nagrywanie		maks. 60 kl./s	
	PAL	maks. 50 kl./s	
Wielozadaniowość	Triplex (nagrywanie, odtwarzanie, LAN)		
Rozdzielczość	wyświetlanie		640 x 448
		PAL	640 x 544
	nagrywanie		640 x 224
		PAL	640 x 272
Format kompresji	Modified MJPEG	normalny	12KB / klatkę
		wysoki	15KB / klatkę
		najwyższy	20KB / klatkę
Dyski HDD	SATA HDD x 1		
Archiwizacja	Na pendrive przez port USB		
Wyszukiwanie	tryb	data, zdarzenie	
	pełny ekran	tak	
Detekcja ruchu	tak		
Utrata sygnału	tak		
Sekwencja	tak		
Brzęczyk	tak		
Regulacja jasności	tak		
Regulacja kontrastu	tak		
Wyjście VGA	640*480/800*600/1024*768/1280*1024		
Nadzorowanie systemu	Automatyczne wznowienie nagrywania po przywróceniu zasilania		
Format transmisji przez LAN	MPEG4		
Zasilanie	DC 12 V / 3A (AC 100 V ~ 240 V 50/60 HZ)		
Wymiary	220 mm x 228 mm x 48 mm (szer. x gł. x wys.)		
Masa	1,5 kg		

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

Detektor wibracji z serii CD400

Detektor uderzeń CD 400 sygnalizuje wszelkie próby sforsowania obiektu za pomocą narzędzi stosowanych z użyciem dużej siły, w skrajnych przypadkach nawet przy użyciu ładunków wybuchowych.

Detektor wykrywa drgania o wysokiej amplitudzie i krótkim czasie trwania. Posiada programowalny licznik zdarzeń. Wyzwolenie alarmu następuje po wystąpieniu zaprogramowanej ilości zdarzeń z przedziału od 1 do 4. Wykrycie eksplozji wyzwala alarm niezależnie od ilości zliczonych zdarzeń.

Detektor można montować na elastycznych, wieloelementowych konstrukcjach, takich jak ramy i ościeżnice okien i drzwi, na ceglanych ścianach, gdzie próby ich sforsowania mogą być dokonane z dużą siłą za pomocą tępego narzędzia.

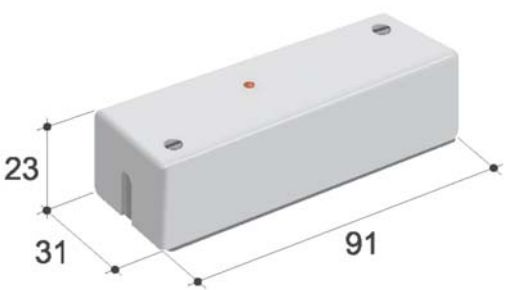
Działanie detektora uderzeń CD 400 jest oparte na cyfrowym przetwarzaniu zarejestrowanych zdarzeń za pomocą mikrokontrolera o zaawansowanym algorytmie obróbki sygnału. Oznacza to niezawodność działania i odporność na zakłócenia z zewnątrz. Detektor posiada wewnętrzny kanał kontrolny do kontroli pracy systemu i wszelkich prób sabotażu oraz wyposażony jest w wewnętrzny rejestrator zdarzeń, "czarną skrzynkę".

Wymaganą czułość detektora można łatwo ustawić przy pomocy potencjometru. W celu sprawdzenia ustawienia czułości należy korzystać z mechanicznego testera CT 400, który generuje drgania podobne do rzeczywistych. Siła generowanych drgań testowych jest zawsze taka sama. W przypadku gdy detektor wykryje atak o dużej sile, wszelkie ustawienia czułości są nieistotne. Detektor jest wyposażony w diodę LED, sygnalizującą alarm i posiada zabezpieczenie przed zdjęciem pokrywy.

Przy instalacji detektora na betonowym lub podobnym podłożu, zalecane jest korzystanie z płyty montażowej MP 400. Przy montażu w zimnych pomieszczeniach lub na wolnym powietrzu, należy skorzystać z wyposażonej w element grzewczy obudowy WH 400, która chroni przed niedogodnymi warunkami atmosferycznymi.

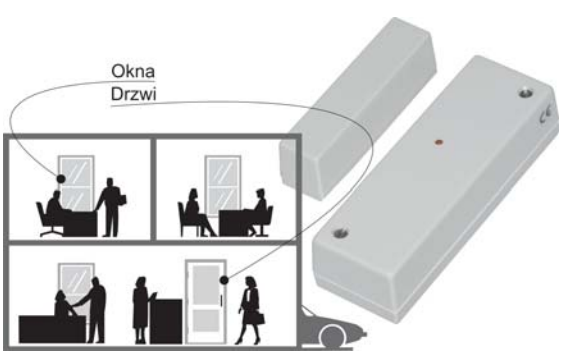
Posiada atest Techom w klasie S.....38/08

Specyfikacja techniczna	
Napięcie zasilania	9-15 V DC
Tętnienia max	2 Vpp
Pobór prądu w stanie czuwania	9 mA
Pobór prądu w stanie alarmu	11 mA
Rodzaj wyjścia alarmowego	przekaźnik
Rezystancja szeregowa pętli zabezpieczającej	20-30 Ohm
Obciążalność	500 mA/35 V
Czas podtrzymania alarmu w trybie AUTO	2 s
Sygnalizacja alarmu w trybie MONITOR	dioda LED
Kasowanie alarmu	wyłączenie zasilania lub zdalny reset na wyjściu D/N
Styk zabezpieczający	NC
Obciążalność	maks. 35 V/50 mA
Temperatura pracy	od -10°C do +70°C
Temperatura przechowywania	od -40°C do +70°C
Wilgotność, DIN 40040	max. 95% RH, klasa F
Kategoria ochronna obudowy IEC 529	IP 31



Materiał	Stal/Drewno/Szkło	Cegła/Gips	Beton*
Zakres	R = 3m	R = 2m	R = 3m

* z użyciem płytki montażowej MP 400



CD 400-R , szczelina 30 mm

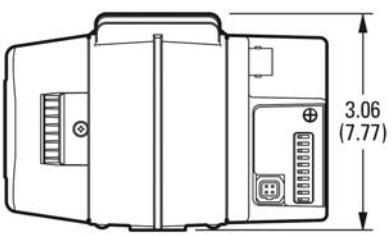
Detektor CD 400 z wmontowany układem kontaktu magnetycznego, chroniącym niezależnym obwodem przed nieuprawnionym otwarciem zabezpieczane okna i drzwi.

ALARMTECH POLSKA Sp. z o.o.
ul. Kielnieńska 115
80-299 Gdańsk – Osowa
tel. (58) 340 24 40, faks (58) 340 24 49
e-mail: info@alarmtech.pl
http://www.alarmtech.pl

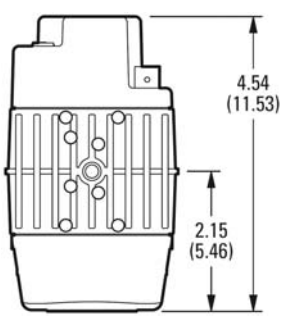
Kamera sieciowa serii IP3701H firmy Pelco

ENDURA ENABLED

Właściwości:
- zasilanie przez sieć Ethernet (IEEE802.3af) lub źródłem zasilania o napięciu 24 VAC,
- architektura otwarta,
- 3 jednoczesne strumienie sygnału wideo:
  - dwa MPEG-4,
  - skalowalny MJPEG,
- protokoły internetowe: TCP, UDP (Unicast, Multicast IGMP) UpnP, DNS, DHCP, RTP, NTP,
- wielopoziomowe zabezpieczenie hasłem,
- EDR (Extended Dynamic Range – rozszerzony zakres dynamiki),
- mocowanie obiektywów C/CS,
- kompensacja oświetlenia tła,
- rozdzielczość pozioma 480 linii TV,
- mocowanie u góry/u dołu, niski profil,
- złącze BNC do celów serwisowych.

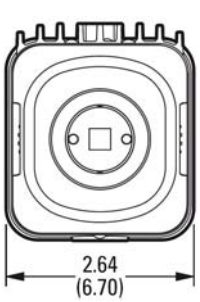


Seria IP3701H to cyfrowe kamery o wysokiej rozdzielczości i czułości przeznaczone do ogólnego stosowania. Dzięki wbudowanemu interfejsowi sieciowemu 100 Base – TX, kamera może wysyłać sygnał wideo bezpośrednio do przeglądarki internetowej (Microsoft® Internet Explorer lub Firefox®) oraz jednocześnie do urządzenia nagrywającego. Jedną z cech kamery jest jej otwarta architektura umożliwiająca podłączenie do urządzeń rejestrujących innych firm. Kamera jest też zgodna z systemem Endura (Endura Enabled™), który umożliwia nagrywanie, zarządzanie, konfigurację oraz oglądanie wielu strumieni wideo jednocześnie.



Po podłączeniu do systemu Endura™, na pracę kamery wpływają technologie EnduraStor™ oraz EnduraView™ umożliwiające optymalizację jakości obrazu i efektywności używanej szerokości pasma. EnduraStor™ znacząco wydłuża czas nagrywania przy mniejszej liczbie klatek/s, natomiast EnduraView™ stale monitoruje i automatycznie reguluje system w celu uzyskania najlepszej możliwej jakości obrazu.

Seria IP3701H jest kompatybilna z interfejsem Pelco IP API, co umożliwia użytkownikowi użytkowanie kamery z oprogramowaniem innych producentów.



Seria IP3701H ma możliwość zasilania bezpośrednio przez przewód sieci Ethernet (PoE IEEE802.3af), redukując tym samym koszt instalacji. Urządzenie posiada również wejście do podłączenia zasilania o napięciu 24 VAC. Kamera wyposażona jest w wyjście wideo BNC umożliwiające przeglądanie obrazu podczas instalacji i konserwacji urządzenia.

Seria kamer IP3701H cechuje się również rozszerzonym zakresem dynamiki bez straty czułości, odwzorowania kolorów, czy też rozdzielczości. Rozszerzony zakres dynamiki umożliwia dostarczenie dobrej jakości obrazu w bardzo trudnych warunkach oświetleniowych.

Uwaga: Wymiary w nawiasach podane są w centymetrach

t.a.c by Schneider Electric

TAC Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa

tel. (22) 313 24 10, faks (22) 313 24 11
e-mail: tac_pol@tac.com
http://www.tac.com/pl

Kamera sieciowa serii IP3701H firmy Pelco

Modele	
IP3701H-2	1/3", kolorowa, cyfrowa kamera o wysokiej rozdzielczości, 480 linii TV, system NTSC
IP3701H-2X	podobnie jak model IP3701H-2, ale działa w systemie PAL

Informacje ogólne	
Urządzenie obrazujące	przetwornik 1/3"
Elementy obrazu IP3701H-2 IP3701H-2X	 768 (Poz) x 494 (Pion) 752 (Poz) x 582 (Pion)
Obszar czułości	6 mm po przekątnej
Rozdzielczość pozioma	480 linii TV
Sterowanie przesłoną	elektroniczne/pasywne
Oświetlenie minimalne	0,5 lx przy f/1.2, 40 IRE, AGC wł., 75% wsp. odbicia
ESC	1/60 – 1/100 000 s
Stosunek sygnał/szum	52 dB (ARW wył.)
Kompensacja oświetlenia tła	wybieralna dzięki ust. przełącznika DIP
System skanowania IP3701H-2 IP3701H-2X	 525 linii, przeplot 2:1 625 linii, przeplot 2:1
Sterowanie przesłoną obiektywu	sterowanie DC/wideo, wybierane przez pozycję przełącznika DIP

Informacje elektryczne	
Porty	RJ-45 złącze dla 100 BASE-TX auto MDI/MDI-X autonegocjacja/ust. ręczne
Typ okablowania	Cat5 lub lepszy dla 100 BASE-TX
Napięcie wejściowe	18 do 30 VAC lub PoE IEEE802.3af klasa 3
Pobór energii	7 W

Informacje mechaniczne	
Montaż obiektywu	mocowanie C/CS (regulowany)
Montaż kamery	mocowanie uchwytu u góry lub u dołu obudowy kamery

Informacje o środowisku pracy	
Temperatura pracy	od -10°C do 50°C
Temp. magazynowania	od -10°C do 70°C

Wideo		
System	NTSC lub PAL	
Kompresja	MPEG-4, MJPEG przy pracy z przeglądarką	
Strumienie wideo	3, jednoczesne	
Rozdzielczość wideo	NTSC	PAL
4CIF	704 x 480	704 x 576
2CIF	704 x 240	704 x 288
CIF	352 x 240	352 x 288
QCIF	176 x 120	176 x 144
Transmisja danych	MPEG-4, 20 kbps do 2 Mpbs na strumień	
Przeglądarka internetowa	podgląd na żywo maksimum 10 źródeł wideo	
Użytkownicy	10 jednoczesnych użytkowników, nieograniczona liczba użytkowników przy wykorzystaniu technologii „multicast"	
Wymagania min. przeglądarki	PC (Mikroprocesor Pentium®4, 1.6 GHz) z systemem Windows®98/Windows 2000/ Windows XP (lub wyższym); Mac®OS X wersja 10.3.9 (lub wyższa) RAM: 512 MB Ethernet: 100 Megabitów Przeglądarka internetowa: Microsoft Internet Explorer 5.5 (lub wyższa), Firefox 1.5 (lub wyższa) Rozdzielczość ekranu: 1024 x 768 pikseli lub wyższa, 16- lub 32- bitowy tryb kolorowy	

Certyfikaty / Wartości znamionowe / Patenty
CE, Klasa B
Certyfikat UL/cUL
Zgodność z IEEE802.3af

Zalecane źródła zasilania	
Serii MCS	Zasilacze 24VAC dla wielu kamer, wewnętrzne
Seria WCS	Zasilacze 24VAC dla jednej/wielu kamer, zewn.

Zalecane uchwyty	
C10-UM	Uchwyt uniwersalny: ścienny /sufitowy

Zalecane obudowy	
EH3512-2	Obudowa zewnętrzna/wewnętrzna, dł. 30,48 cm (12"), zawierająca grzałkę, wentylator i odszraniacz, zasilanie 24VAC.
EH4718-2	Obudowa zewnętrzna/wewnętrzna, dł. 45,72 cm (18"), zawierająca grzałkę i wentylator, zasilanie 24VAC.
EH4722-2	Obudowa zewnętrzna/wewnętrzna, dł. 55,88 cm (22"), zawierająca grzałkę i wentylator, zasilanie 24VAC.

Uwaga: temperatura wewnątrz obudowy nie może przekraczać zakresu temperatur pracy kamery IP3701H.

t.a.c by Schneider Electric

TAC Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa

tel. (22) 313 24 10, faks (22) 313 24 11
e-mail: tac_pol@tac.com
http://www.tac.com/pl

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

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

---

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

AAT TRADING COMPANY Sp. z o.o.
ul. Puławska 431
02-801 Warszawa
tel. (22) 546 05 46
faks (22) 546 05 01
e-mail: aat_wawa@aat.pl
www.aat.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ul. Os. Na Murawie 10/2, 61-655 **Poznań**
tel. (32) 790 76 37
faks (32) 790 76 70
e-mail: poznan@e-alpol.com.pl

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

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

ul. Modzelewskiego 35/U9
02-679 **Warszawa-Mokotów**
tel. (32) 790 76 34
faks (32) 790 76 69
e-mail: warszawa@e-alpol.com.pl

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

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

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

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

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

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

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

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

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

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

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

---

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

LEGRAND POLSKA Sp. z o.o.
Al. Wyścigowa 8
02-681 Warszawa
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrand.pl

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

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

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

CCX
ul. Ligocka 103
Budynek 9.2
40-568 Katowice
tel. (32) 609 90 80
faks (32) 609 90 81
e-mail: biuro@ccx.pl
www.ccx.pl

Centrum Monitorowania Alarmów
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 0 888
faks (22) 546 0 619
e-mail: warszawa@cma.com.pl
www.cma.com.pl

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

ul. Na Niskich Łąkach 26, 50-422 **Wrocław**
tel. (71) 340 0 209
faks (71) 341 16 26
e-mail: wrocław@cma.com.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

EUREKA SOFT & HARDWARE
Rynek 13
62-300 Września
tel. (61) 437 90 15
faks (61) 436 27 14
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

P.W. IRED
Kazimierzówka 9
21-040 Świdnik
tel. (81) 751 70 80
tel. kom. (0) 605 362 043
faks (81) 751 71 80
e-mail: ired@exe.pl
www.ired.com.pl

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

KABE Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 32 48 900
faks (32) 32 48 901
e-mail: handel@kabe.pl
www.kabe.pl, www.kabe.eu

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

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

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

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

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

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

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. (75) 755 78 78, 642 45 35
faks (75) 642 45 25
e-mail: info@micronix.pl
www.micronix.pl

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

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

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

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

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

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

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

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

Przedstawicielstwo:
ul. Grunwaldzka 119, 60-313 **Poznań**
tel. (61) 657 93 60
poznan@omc.com.pl

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

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

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

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

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

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

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

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

POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV
ul. Obornicka 276
60-693 Poznań
tel./faks (61) 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl

PROXIMA Sp. J.
ul. Filtrowa 23
87-100 Toruń
tel. (56) 660 20 00
faks (56) 660 20 03
e-mail: proxima@proxima.pl
www.proxima.pl

Filia: (alarmy do obiektów)
ul. Olbrachta 4/6
87-100 **Toruń**
tel. (56) 661 18 96
faks (56) 661 18 97
e-mail: alarmy@proxima.pl

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

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

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

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

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

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

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

SATIE
ul. Łączyny 3
02-820 Warszawa
tel./faks (22) 314 69 50
e-mail: info@acie.pl
www.acie.pl

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

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

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

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

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

S.M.A.
System Monitorowania Alarmów Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. (22) 651 88 61
faks (22) 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ul. Inowrocławska 39C, 53-649 **Wrocław**
tel. (71) 348 44 64
faks (71) 348 36 35
e-mail: wroclaw@spstrading.com.pl
ul. Inflancka 6, 91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.com.pl

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

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

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

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

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

TAC Sp. z o.o.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TYCO FIRE AND INTEGRATED SOLUTIONS Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 8 301
faks (22) 430 8 302
e-mail: tycofis-pl@tycoint.com
www.tycofis.pl

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

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

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

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

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

DZIAŁALNOŚĆ

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

DZIAŁALNOŚĆ

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

KATEGORIE

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

KATEGORIE

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

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk
teresa@zabezpieczenia.com.pl
Redaktor merytoryczny
Adam Bułaciński
adam@zabezpieczenia.com.pl
Dział marketingu i reklamy
Ela Końka
ela@zabezpieczenia.com.pl
Redaguje zespół:
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Ireneusz Krysowaty
Paweł Niedziejko
Edward Skiepko
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz
Współpraca zagraniczna
Rafał Niedzielski
rafal@zabezpieczenia.com.pl
Współpraca
Marcin Pyclik
Sławomir Wagner
Andrzej Wójcik
Skład i łamanie
Marek Bladoszewski
Korekta
Paweł Karczmarzyk
Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. (22) 546 09 51, 53
faks (22) 546 09 59
www.zabezpieczenia.com.pl
Wydawca
AAT Trading Company Sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 05 97
faks (22) 546 05 29
Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Cennik reklam

Reklama wewnątrz czasopisma:

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

Artykuł sponsorowany:
indywidualne negocjacje (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

Reklama na okładkach:

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

Spis teleadresowy:

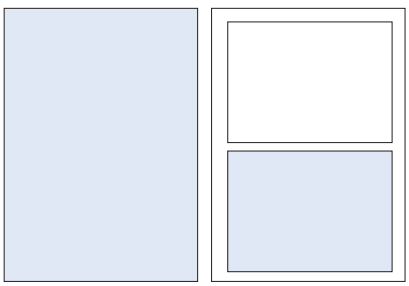
jednorazowy wpis	70 zł

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji

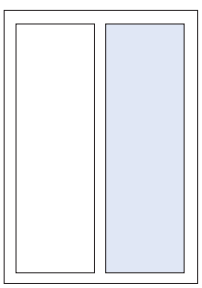
W przypadku zamówienia na 12 emisji 10% rabat

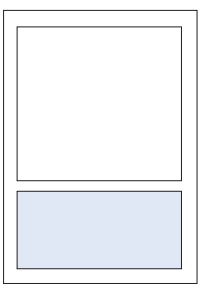
Podane ceny nie uwzględniają podatku VAT (22%)

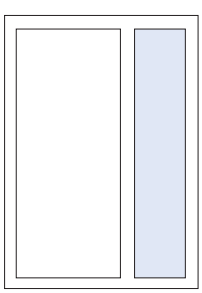
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej **http://www.zabezpieczenia.com.pl** w dziale **Reklama**

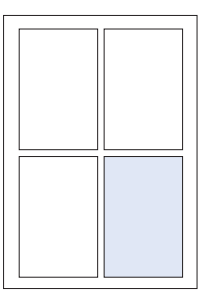

cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)


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


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


1/3 strony
(53 x 257 mm)


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

Spis reklam

MP 508

INTERAKTYWNY, MULTIMEDIALNY, ZDALNIE STEROWANY SYSTEM ALARMOWY

pełne zarządzanie systemem przez telefon/GSM
nowe oprogramowanie PC *Hi-Connect*
funkcje weryfikacji alarmów za pomocą CCTV
funkcje kontroli dostępu

- 64 linie alarmowe
- 27 wyjść programowalnych
- 8 stref
- 4 grupy stref
- 8 klawiatur
- 16 czytników kluczy
- 32 kody użytkowników
- 32 klucze elektroniczne i zbliżeniowe
- 1000 zdarzeń w pamięci

ELKRON

MIWI-URMET Sp. z o. o.
91-341 Łódź, ul. Pojezierska 90 A, tel. 042 616 21 00, fax 042 616 21 13
www.miwiurmet.com.pl, e-mail: miwi@miwiurmet.com.pl

urmet MIWI

Multitechnologiczne rozwiązanie zapewniające łatwą migrację.

Przy wykorzystaniu technologii 13.56 MHz HID jest naprawdę godnym polecenia wyborem. Linia produktów SmartID™ obejmuje wszystkie inteligentne technologie, niezależnie od tego, czy mówimy o iCLASS®, DESFire® lub MIFARE®. SmartID zapewnia elastyczne rozwiązanie wysokich częstotliwości umożliwiające Ci migrację w Twoim własnym tempie. Wszystkie produkty HID posiadają dożywotnią gwarancję i dlatego zaufało nam tak wiele przedsiębiorstw. Nie wierz nam tylko na słowo. Wypróbuj nas! Skontaktuj się z nami, aby uzyskać więcej informacji: mediaemea@hidglobal.com.

hidglobal.com

HID

ACCESS technology.