CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 5(63)/2008

ZABEZPIECZENIA

10 lat za nami

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

W NUMERZE:

NASTĘPNA GENERACJA SYSTEMÓW ZABEZPIECZEŃ PRZYBYŁA

FIKCJA STAŁA SIĘ FAKTEM ...
SYSTEMY ZABEZPIECZEŃ I-PRO PANASONIC.

Panasonic opanował najnowszą technologię IP, aby stworzyć naprawdę futurystyczny system zabezpieczeń i-pro, zawierający pełną gamę produktów. Pozwala on powstrzymać nie tylko inwazję intruzów, ale także znacząco redukuje koszty związane z użytkowaniem systemu, między innymi poprzez zmniejszenie ilości kabli oraz kosztów obsługi. Ponieważ posiadamy specjalistyczną wiedzę w tej dziedzinie, jesteśmy w stanie zaproponować najlepsze z możliwych rozwiązań.

Więcej informacji o produktach i-pro uzyskasz pod numerem telefonu (22) 33 81 177
lub odwiedzając stronę pss.panasonic.eu

i-pro

Panasonic
ideas for life

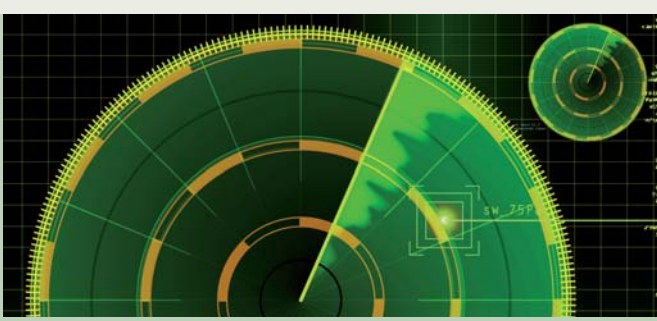
Spis treści

CZASOPISMO ZABEZPIECZENIA 5/2008

Phishing – polowanie na łatwowiernych (część I) 22

Niebezpieczeństwa płynące z sieci wewnętrznej korporacji – sposób obrony 31

Wymagania w zakresie bezpieczeństwa okien i drzwi wynikające z norm europejskich 44



Wykorzystanie radarów w ochronie zewnętrznej obiektów 77

Ośrodek Szkoleniowy PISA zaprasza na **kursy i seminaria:**

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

Seminaria adresowane są do osób, które ukończyły stosowne kursy w innych Ośrodkach Szkoleniowych.

Absolwenci kursów i seminariów otrzymują dwa dokumenty wystawione bezterminowo:
– zaświadczenie o ukończeniu kursu (druk MEN),
– dyplom OS PISA.

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

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

Bezpośr. inf. PISA

Bosch Security Systems oraz **CNBOP**
zapraszają na szkolenie

Bosch Security Systems razem z **Centrum Naukowo-Badawczym Ochrony Przeciwpożarowej** podejmują wspólną inicjatywę **szkoleń SAP i DSO** dedykowanych dla projektantów, instalatorów i konserwatorów.

Bosch Security Systems nieustannie potwierdza jakość swoich produktów poprzez kolejne certyfikaty Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej. Zależy nam również na bezbłędnych i spełniających najwyższe standardy instalacjach. Dlatego od wielu lat prowadzimy szkolenia w ramach naszej firmy. W tym roku postanowiliśmy połączyć siły z CNBOP i zaplanowaliśmy wspólne szkolenia dedykowane dla projektantów, instalatorów i konserwatorów systemów sygnalizacji alarmu pożarowego (SAP), a także dźwiękowych systemów ostrzegawczych (DSO). Szkolenia będą innowacyjną formą łączącą teorię z praktyką.

Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej i firma Bosch Security Systems organizują:
– **szkolenie** dla projektantów, instalatorów i konserwatorów **systemów sygnalizacji alarmu pożarowego**, które odbędzie się w dniach **21, 22 oraz 30 października 2008 r.**,
– **szkolenie** dla projektantów, instalatorów i konserwatorów **dźwiękowych systemów ostrzegawczych**, które odbędzie się w dniach **23, 24 oraz 31 października 2008 r.**

CNBOP i firma Bosch zapraszają do udziału, liczba miejsc ograniczona.

Bezpośr. inf. Bosch Security Systems

PRAGOALARM/PRAGOSEC 2009
– targi zabezpieczeń w Republice Czeskiej

Siedemnasta edycja międzynarodowych targów zabezpieczeń PRAGOALARM/PRAGOSEC 2009, które obecnie są organizowane w cyklu dwuletnim na terenie wystawienniczym Incheba Expo w Pradze (*Výstavišti Incheba Expo Praha*), odbędzie się w dniach od 24 do 26 lutego 2009 roku.

Struktura, zamierzenia i nowa data targów powinny z jednej strony umożliwić wystawcom zaprezentowanie ostatnich innowacji, produktów i usług na początku sezonu, a z drugiej – dostarczyć profesjonalistom z branży zabezpieczeń obszernych informacji na temat trendów rozwoju w zakresie sprzętu, systemów i instalacji zapewniających bezpieczeństwo (PRAGOALARM) oraz ochrony przeciwpożarowej i sprzętu ratowniczego (PRAGOSEC).

Organizatorzy targów przygotowali dla ich uczestników następujące nowości:

- ulepszoną i uproszczoną nomenklaturę targów (zob. materiały na www.pragoalarm.cz),
- równoległą wystawę „Panelowe budynki i mieszkania” („*Panelový dům a byt*”), dotyczącą rewitalizacji, rekonstrukcji, finansowania, ze szczególnym uwzględnieniem systemów dociepleń, wind i elewacji, czynną w czwartek 26 lutego 2009 r.,
- równoległą wystawę „Okna – Drzwi – Schody” *(„Okna – Dveře – Schody”)*, czynną także w czwartek 26 lutego 2009 r.,
- program towarzyszący (w przygotowaniu) – konferencje międzynarodowe, debaty profesjonalistów, prezentacje, pokazy i konkursy firmowe,
- centrum doradcze dla wystawców zagranicznych (pomoc w kontaktach z partnerami biznesowymi i w zakresie wyjaśniania zasad przedsiębiorczości w dziedzinie bezpieczeństwa informacji i obiektów oraz ochrony fizycznej),
- program spotkań towarzyskich.

Oficjalny termin nadsyłania zgłoszeń dla wystawców to **30 października 2008 r.** (rozmieszczanie stoisk rozpoczęło się już w sierpniu 2008 r.).

Źródło: bezpośr. informacja firmy Incheba Praha oraz www.pragoalarm.cz/www.pragosec.cz

Ogólnopolska Wystawa Monitoringu Wizyjnego ALARM 2008

W dniach **5–6 listopada** br. odbędzie się w Kielcach w pawilonach targowych Targów Kielce **Konferencja** (5 listopada) i **Wystawa Monitoringu Wizyjnego „ALARM”**.

W halach wystawienniczych kieleckiego ośrodka firmy zaprezentują najnowsze rozwiązania i technologie z zakresu szeroko pojętego bezpieczeństwa, ale dominującą tematyką targów będzie, zgodnie z założeniem organizatorów, monitorig wizyjny.

Swoją ofertę przedstawią również firmy detektywistyczne i agencje ochrony, a także firmy ubezpieczeniowe.

Podobnie jak w ubiegłych latach, targom ALARM towarzyszyć będzie **Ogólnopolska Konferencja „Bezpieczne Miasto – Monitoring Wizyjny Miast”**. Jest ona jednym z elementów programu „Bezpieczne Miasto”, wprowadzanego sukcesywnie przez Komendę Główną Policji w największych miastach Polski. Celem programu jest zabezpieczenie najbardziej zagrożonych przestępczością obszarów zurbanizowanych oraz poprawa poczucia bezpieczeństwa ich mieszkańców. Jak bowiem dowodzą badania, w strefach rejestrowanych za pomocą kamer zmniejsza się liczba popełnianych przestępstw.

W konferencji udział wezmą miejscy i powiatowi komendanci policji, straży pożarnej, burmistrzowie miast, przedstawiciele urzędów miast, policji, straży miejskich, firm i instytucji zajmujących się bezpieczeństwem. Przekażą oni informacje dotyczące wdrażania systemów bezpieczeństwa i efektywnego z nich korzystania.

Równolegle z targami ALARM odbędzie się **Wystawa Wyposażenia i Budowy Obiektów Sportowych „SPORT-OBIEKT”**. Towarzysząca wystawie konferencja będzie poświęcona między innymi nowym trendom w budownictwie obiektów sportowych oraz sposobom ich zabezpieczania.

W tym roku najważniejszym wydarzeniem towarzyszącym wystawie SPORT-OBIEKT będzie **Międzynarodowa Konferencja „Bezpieczny Stadion”**, która odbędzie się w dniu 6 listopada 2008 r. Organizatorem konferencji jest Polski Związek Piłki Nożnej. Jest ona elementem ogólnonarodowej kampanii na rzecz poprawy bezpieczeństwa, a także estetyki i komfortu w obiektach sportowych, a jej tematem jest modernizacja i zwiększanie bezpieczeństwa obiektów sportowych w Polsce.

Więcej informacji o targach ALARM na stronie www.alarm.targikielce.pl.

Redakcja

Zapraszamy na targi CARTES & IDentification 2008

Najważniejsze światowe targi zabezpieczeń cyfrowych i inteligentnych technologii odbędą się w dniach od 4 do 6 listopada 2008 r. na terenie Parc des Expositions Paris-Nord Villepint.

Po sukcesie odniesionym w ubiegłym roku targi **CARTES & Identification** przygotowują się do tegorocznej edycji, która z pewnością ponownie przyciągnie ponad 20000 zwiedzających. Organizatorzy oczekują również udziału 520 wystawców i 1700 uczestników kongresu. Uznane na całym świecie za punkt odniesienia dla branży zabezpieczeń cyfrowych i inteligentnych technologii targi CARTES & Identification stanowią niewątpliwie światowe forum tej branży. W dniach od 4 do 6 listopada bieżącego roku wszyscy specjaliści związani z kartami chipowymi i identyfikacją ponownie spotkają się w Paryżu na terenach wystawowych Paris-Nord Villepinte.

Tematy przewodnie edycji 2008: transakcje elektroniczne, **zarządzanie identyfikacją** (*ID management*). Gość honorowy imprezy: Stany Zjednoczone.

Po Japonii, w tym roku gościem honorowym targów CARTES & IDentification będą Stany Zjednoczone. Jako prawdziwy prekursor w dziedzinie zastosowań transportowych, płatniczych, lojalnościowych i z zakresu wymiany Stany Zjednoczone skupią się głównie na rozwiązaniach bezdotykowych.

Wobec wzrostu znaczenia technologii bezdotykowych w Europie Stany Zjednoczone wydają się bardzo zaawansowane w rozwijaniu ich licznych zastosowań, takich jak na przykład dokumenty elektroniczne lub karty płatnicze.

Rynek bezpiecznych transakcji elektronicznych jest strategiczną dziedziną, w której USA działają bardzo aktywnie i w związku z tym mają tendencję do narzucania nowych norm technologicznych.

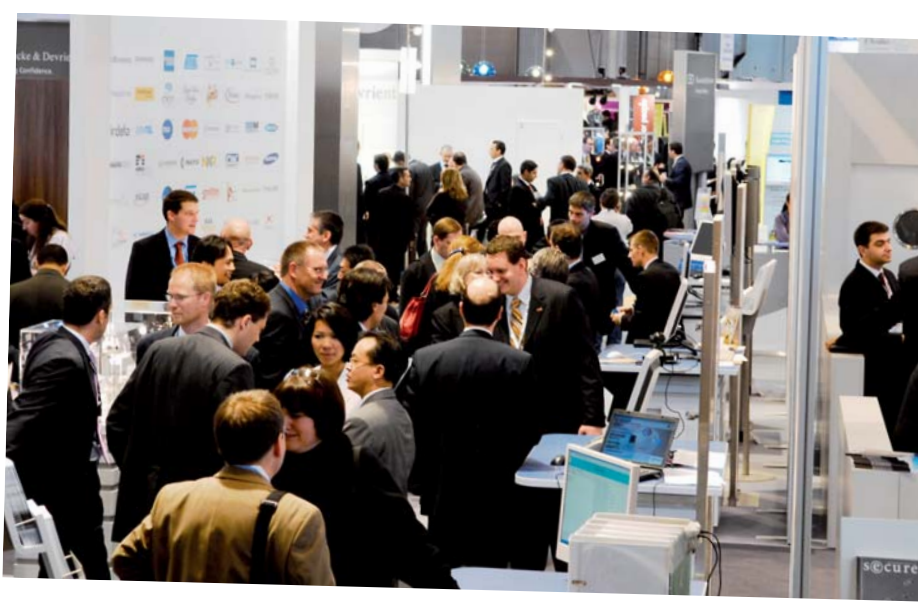
Swoją obecność podczas najbliższej edycji targów Stany Zjednoczone zaznaczą wystąpieniami podczas kongresu, pawilonem narodowym zlokalizowanym w samym centrum targów, imprezami towarzyszącymi i obecnością ważnych decydentów.

Centralnym punktem targów IDentification będzie *ID management*

Targi CARTES 2008 rezerwują szczególne miejsce dla wyjątkowo dynamicznego sektora, jakim jest identyfikacja. Potwierdza to fakt, że w ubiegłym roku z powodzeniem wprowadzono ekspozycję o nazwie Identification. Poświęcona technologiom zabezpieczeń i biometrii, w tym roku zlokalizowana będzie obok targów CARTES i skierowana do tej samej grupy zwiedzających.

Targi zgromadzą wszystkie podmioty oferujące rozwiązania i technologie związane z biometrią, zabezpieczaniem dokumentów, uwierzytelnianiem, kontrolą dostępu fizycznego i logicznego, kryptografią, technologiami RFID i procedurami *e-Government*.

Jednym z głównych tematów tegorocznej edycji targów będzie zarządzanie certyfikatami elektronicznymi. Wystawcy zaprezentują rozwiązania odpowiadające obecnym potrzebom w dziedzinie zabezpieczeń. Obecność na targach IDentification będzie zatem niezbędna do zdobycia informacji o rozmaitych technologiach w zakresie *ID management*.



Po ubiegłorocznym sukcesie organizatorzy targów CARTES & IDentification również w tym roku przygotowują ekspozycję Mobile Transaction TechZone przy współpracy z NFC Forum.

Stymulowane rozwojem technologii bezdotykowych i multiaplikacyjnych transakcje mobilne oferują rozmaitym podmiotom nowe zastosowania i nowe perspektywy: NFC, RFID, M2M, bezpieczeństwo transakcji, *kiosk technologies*.

W roku 2007 w tej części ekspozycji obecne były takie firmy, jak : Innovision, Legic, MasterCard, Nexpert, Nokia, NXP Semiconductors, Stolpan, Toppan Printing, USA Technologies. W roku bieżącym pojawią się nowe, równie dynamiczne podmioty.

CARTES & IDentification 2008 to również:

1. **Kongres** o niewątpliwie największym światowym znaczeniu, będący skondensowanym źródłem informacji i *know-how*. Trzydniowy kongres będzie międzynarodowym forum wymiany doświadczeń i wiedzy o nowościach. Spotkanie to, poświęcone tematyce związanej z kartami i identyfikacją, stanowić będzie najlepsze odbicie tendencji rynku i niezbędne uzupełnienie wizyt na stoiskach. Konferencje prezentujące najbardziej innowacyjne projekty będą okazją do wymiany opinii, spotkań prelegentów-ekspertów z ponad 1700 uczestnikami kongresu oraz do omówienia najbardziej aktualnych tematów.
2. **Inauguracyjna konferencja World Card Summit**. Zgromadzi ona czołowe przedsiębiorstwa branży, których przedstawiciele wymienią poglądy na temat aktualnego stanu rynku oraz jego wizji.
3. **Konkurs z nagrodami – Sezamami** (*SESAMES Awards*) – będącymi przejawem uznania w branży. Bardzo pożądane przez specjalistów z dziedziny kart chipowych i identyfikacji nagrody SESAMES są wyrazem międzynarodowego uznania ze strony branży. Konkurs jest otwarty dla wszelkich przedsiębiorstw z reprezentowanych sektorów, niezależnie od tego, czy biorą one udział w targach CARTES & IDentification w charakterze wystawców, czy też nie. Jako wyjątkowe narzędzie promocji dla innowacyjnych projektów nagrody stanowią uwieńczenie wielu lat prac badawczo-rozwojowych. Sezamy są przyznawane przez jury złożone z ekspertów i wręczane podczas prestiżowej ceremonii organizowanej w Paryżu w przeddzień otwarcia targów. Z produktami zakwalifikowanymi do finału konkursu można się będzie zapoznać na terenie ekspozycji pod nazwą SESAMES, znajdującej się w centralnej części targów.

Już teraz zaznaczcie Państwo w kalendarzu termin 4, 5 i 6 listopada 2008 r.! Najnowsze informacje na temat targów CARTES & IDentification są dostępne na stronie internetowej www.cartes.com.

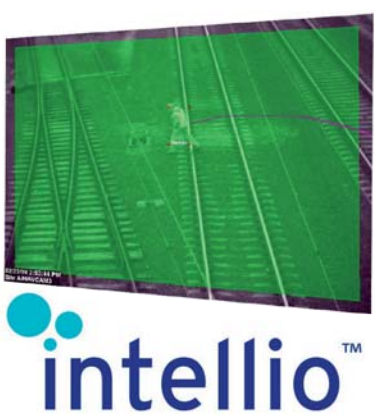
Informacje praktyczne:

Termin: 4, 5 i 6 listopada 2008 r.

Miejsce: teren Parc des Expositions Paris-Nord Villepinte w Paryżu

Bezpośr. inf. Ewa Zielińska
UBIFRANCE
Misja Ekonomiczna Ambasady Francji
e-mail: ewa.zielinska@missioneco.org

Intellio zabezpiecza kable miedziane dla kolei węgierskich



Miedziane kable zapewniające bezpieczeństwo ruchu kolejowego (służące do sterowania ruchem oraz prędkością pociągów – przyp. red.) w najważniejszych węzłach międzynarodowej linii Wiedeń – Budapeszt są strzeżone przez **inteligentne kamery IP** z wbudowaną **detekcją intruza**. Kradzieże kabli związanych z **bezpieczeństwem transportu** mogą powodować nie tylko wielkie straty materialne, ale i zagrożenie życia ludzkiego.

– *Głównym celem projektu było umożliwienie złapania napastnika, zanim dokona on kradzieży, i uniknięcie zniszczeń. Przez unikanie takich sytuacji można ochronić życie ludzkie i zaoszczędzić miliony euro* – powiedział **János Kópházi**, szef **Intellio**.

Nowy system **MÁV** (węgierskich państwowych kolei osobowych – przyp. red.) jest zupełnie inny niż zwykle stosowane rozwiązania zabezpieczeń. Ostatnio zainstalowany system zapewnia **detekcję intruza**, co w przypadku naruszenia bezpieczeństwa powoduje natychmiastowe wysłanie alarmu do biura ochrony. Zastosowane **kamery o megapikselowej rozdzielczości** są w stanie odróżnić ludzi od zwierząt lub innych poruszających się obiektów. Ochrona ma za zadanie reagować tylko wtedy, gdy na obserwowany obszar przedostają się ludzie.

Samodzielne punkty obserwacyjne (inteligentne kamery IP) komunikują się między sobą przez sieć WLAN. Zapis megapikselowych strumieni wizyjnych odbywa się dzięki tej samej sieci bezprzewodowej, która jest wykorzystywana do przesyłania danych.

Monitorowanie i przyjmowanie alarmów jest realizowane w centralnym biurze ochrony. Przesył danych z obserwowanych miejsc odbywa się przy wykorzystaniu technologii **GSM UMTS 3G**.

Wszystkie kamery są wyposażone w przystosowany do trudnych warunków pracy **reflektor podczerwieni**, używany do obserwacji w dzień i w nocy, co umożliwia monitorowanie na odległość 40–70 metrów.

– *Efektywność zwykłych systemów dozoru bazuje dziś na elemencie ludzkim. Systemy te nie spełniają żadnej innej roli poza transmisją obrazów do operatorów. Od operatorów takich wielokamerowych systemów wymaga się, aby przez długi czas wykazywali czujność i rozpoznawali na wielu ekranach zdarzenia związane z bezpieczeństwem. Takie rozwiązanie pociąga za sobą jednak mnóstwo błędów ludzkich i w większości przypadków ochrona może reagować dopiero po zaistnieniu szkód, w wyniku analizy zarejestrowanego materiału wizyjnego* – powiedział János Kópházi i dodał – *co gorsza, jakość obrazu jest często niewystarczająca do tego, aby zidentyfikować intruzów*.

– *Technologia wykorzystywana przez MÁV oferuje wiele pionierskich rozwiązań w obszarach związanych z bezpieczeństwem, takich jak zabezpieczanie obrazów w galeriach, monitorowanie ruchu ulicznego czy rozwiązania dla handlu detalicznego* – podsumował p. Kópházi.

Więcej informacji – na www.intellio.eu.

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

Nowa strona www.satel.pl

Konsekwentnie budując nowoczesny wizerunek, firma **SATEL** zdecydowała się na całkowitą przebudowę swojej internetowej wizytówki, którą jest witryna www.satel.pl. Zmiany objęły nie tylko szatę graficzną, czyniąc nową stronę bardziej czytelną i dynamiczną, ale także wprowadzenie nowej formy nawigacji.

Wśród najważniejszych nowości wymienić należy funkcję wyszukiwania, ułatwiającą dotarcie do żądanej treści – zarówno informacji o produkcie, jak i powiązanych z nim dokumentów czy oprogramowania. Kolejnym udogodnieniem jest dopracowanie systematyki produktów – dzięki nowemu sposobowi ich skatalogowania odnalezienie interesującego nas urządzenia staje się bardzo proste. Dodatkowo każdy z produktów posiada własną kartę katalogową w formacie PDF, zawierającą opis ogólny produktu, jego właściwości i dane techniczne, jak również duże zdjęcie.

Wraz z wprowadzeniem gruntownych zmian do witryny www.satel.pl usystematyzowany został również zestaw informacji o produktach – celem tego działania było ułatwienie doboru sprzętu z szerokiej oferty firmy.

Zestaw informacji o produktach uzupełniony będzie w najbliższym czasie przez prezentacje multimedialne, ułatwiające poznanie funkcjonowania wybranych urządzeń.

Serdecznie zapraszamy!

Bezpośr. inf. Satel

Siemens przejmuje MAC Systems

Siemens Building Technologies przejmuje 100% udziałów w firmie MAC Systems, mieszczącej się w Canton w stanie Massachusetts (USA). W ten sposób wzmacnia swoją pozycję na rynku **kontroli dostępu i systemów zarządzania bezpieczeństwem** w regionie Nowej Anglii (obejmującym sześć amerykańskich stanów: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island i Vermont – przyp. red.).

Od roku 1981 firma MAC Systems należała do czołowych graczy na regionalnym rynku elektronicznych systemów zabezpieczeń. Poza telewizją dozorową i systemami zapisu wizyjnego specjalizowała się zarówno w **optycznych**, jak i w **biometrycznych systemach kontroli dostępu**.

Odbiorcami produktów MAC Systems były centra badawcze, uniwersytety, obiekty rządowe o dużym poziomie zabezpieczeń oraz budynki o przeznaczeniu handlowym. Obecnie firma zatrudnia 60 osób i ma wielu klientów w regionie Nowej Anglii.

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

Bosch tworzy globalne partnerstwo z NetApp

Bosch Security Systems i **NetApp** (Network Appliance Inc. z USA) stworzyły globalne partnerstwo. Zgodnie z podpisaną umową Bosch będzie sprzedawać i wspierać pod wspólną marką urządzenia pamięciowe NetApp jako część swojego portfolio w zakresie CCTV. Bosch Security Systems jest firmą działającą w branży systemów zabezpieczeń na całym świecie, NetApp jest zaś twórcą innowacyjnych rozwiązań pamięciowych oraz służących do zarządzania danymi. Umowa jest strategicznym ruchem w związku z utrzymującym się gwałtownym rozwojem rynku telewizji dozorowej IP.

– *Rynek ciągle dojrzewa w swoim rozumieniu architektury wizyjnych systemów IP, czego rezultatem jest znaczący stopień przyjęcia się na nim podejścia firmy Bosch w zakresie zapisu wizyjnego – kierowania strumienia wideo bezpośrednio do macierzy RAID lub pamięci sieciowych i eliminacji sieciowych rejestratorów wizji* – powiedział Johan Jubbega, wiceprezes Global Video Systems and Products w firmie Bosch Security Systems.

Firma Bosch była pionierem w rozwoju kamer IP i koderów kierujących strumień wizyjny bezpośrednio do macierzy RAID lub pamięci sieciowych (SAN – ang. *Storage Area Network*). To nagradzane i efektywne podejście stało się możliwe dzięki bazującemu na IP standardowi pamięciowemu *Internet Small Computer System Interface* (iSCSI). Dzięki umowie o partnerstwie Bosch powiększa asortyment swoich produktów o trzy urządzenia NetApp wykorzystujące protokół iSCSI. Produkty te obejmują serię FAS2000 – skalowalne i efektywne pod względem kosztów urządzenia zapewniające pamięć do 65 TB, a także S550 – urządzenia pamięciowe do małych i średnich zastosowań, które zostały ostatnio nagrodzone przez czasopismo *Windows IT Pro* (2007 Editors' Best Award).

– *To właściwy czas na partnerstwo z Bosch zgodne z oczekiwaniami dotyczącymi rozwiązań telewizji dozorowej IP, które pojawiły się wśród klientów* – powiedział Andreas König, szef i wiceprezes EMEA w NetApp. – *Dzięki rozwiązaniom NetApp, które wykorzystują protokół iSCSI, i połączeniu ich z produktami Bosch klientom zapewnia się sprawdzoną i efektywną odpowiedź na ich potrzeby w zakresie podglądu wizyjnego.*

Zgodnie z warunkami umowy NetApp będzie towarzyszyć partnerom firmy Bosch we wsparciu przedsprzedażowym produktów o wspólnej marce. Firma zapewni także szkolenia i certyfikację grup wsparcia technicznego Bosch. Z kolei Bosch zapewni klientom techniczne wsparcie posprzedażowe w zakresie urządzeń pamięciowych.

Aby zapewnić nieprzerwaną kompatybilność produktów, Bosch wzmocni swój wgląd w „mapę drogową" technologii NetApp. Wprowadzaniu zmian w produktach telewizji dozorowej Bosch będzie towarzyszyć wczesny dostęp specjalistów tej firmy do urządzeń NetApp, tak aby można było skorzystać z nowych właściwości i funkcji, które pojawią się dla produktów z przyszłej oferty NetApp.

Źródło: www.securityworldhotel.com
Tłumaczenie: Adam Bułaciński

Spectra IV IP
– kamera obrotowa Pelco w sieci

W lipcu firma **Pelco** wprowadziła do sprzedaży system kamerowy **Spectra IV IP**, kolejny wariant swojego docenianego na całym świecie produktu. Jest to dualny **system kamerowy PTZ**, który może pracować w instalacji analogowej i cyfrowej IP. Spectra IV IP zawiera wszystkie rozbudowane funkcje analogowej Spectry IV, łącznie z analogowym wyjściem wideo i sterowaniem. Jednocześnie możliwe jest podłączenie do sieci IP i przesyłanie wideo i sterowania PTZ w postaci cyfrowej. Odbiornikami strumieni wideo ze Spectry IP mogą być rejestrator DVR5100 w wersji 1.5, systemy Integral Digital Sentry (wkrótce) lub inny system albo oprogramowanie, którego producent zaimplementował dostarczany przez Pelco protokół. Do grupy firm, które współpracują z Pelco w tym zakresie, należą m.in.: Milestone Systems, ObjectVideo, OnSSI, Plustek, Visual Demence i Lenel Systems International. Spectra IV IP jest oczywiście zgodna z systemem dystrybucji wideo w sieciach IP Endura, który jest rozwijany przez Pelco. Kamera ma wbudowany serwer wideo, strumień MJPEG może być odbierany przez przeglądarkę internetową Internet Explorer lub Mozilla Firefox.

Spectra IV IP jest dostępna w kilku wersjach obudowy: wewnętrznej do montażu w suficie na wysięgniku, zewnętrznej do montażu w suficie na wysięgniku oraz w wykonaniu wzmocnionym i stalowym. Mogą być stosowane moduły kamerowe w wersji dzień – noc ze zbliżeniem 35x, 23x i 18x oraz w wersji kolor 22x i 16x. Kopuły, tak jak w poprzednich modelach Spectry, mogą być przeźroczyste, przyciemnione, chromowane albo złocone.

Produkt spotkał się z bardzo dużym zainteresowaniem podczas ostatnich targów IFSEC w Birmingham, gdyż w wielu krajach system Spectra jest uważany za wzorcowy.

W Polsce produkty Pelco są dostępne w sieci Partnerów firmy **TAC**, która jest wyłącznym przedstawicielem firmy Pelco w Polsce.

Bezpośr. inf. TAC

Wytrzymały **monitoring wizyjny** w ofercie **Veracomp**

Firma **Veracomp** wprowadziła do oferty nowe kamery firm **Bosch Security Systems**, **Forward Vision** i **Extreme CCTV**. Urządzenia służą do monitoringu wizyjnego prowadzonego w warunkach ekstremalnych.

Sprzęt wyróżnia wyjątkowa wytrzymałość na niską i wysoką temperaturę, antywybuchowość, wandaloodporność oraz dobre właściwości obserwacji nocnej. Kamery przeznaczone są do pracy w obiektach komercyjnych i przemysłowych o podwyższonym ryzyku, w tym m.in. w więzieniach, szpitalach, zakładach petrochemicznych czy portach morskich. Gama oferowanych przez Veracomp produktów obejmuje również systemy rozpoznawania tablic rejestracyjnych oraz oświetlacze IR Derwent.

Model EX30 z przetwornikiem 570 TVL CCD z mechanicznym filtrem IR, wyposażony w obiektyw 5–50 mm z korekcją IR i technologię IR Black Diamond daje możliwość detekcji z odległości do 100 m. Kamera nadaje się do ochrony obwodowej, wymagającej wysokiej jakości obrazu w obiektach komercyjnych i przemysłowych.

Kamera dualna IR o wysokiej rozdzielczości EX82 posiada dwa przetworniki CCD 570 TVL kolor/mono, daje wyraźny obraz w kolorze w dzień i mono w nocy. Wykorzystuje technologię IR Black Diamond i umożliwia detekcję z odległości do 75 m. Typowe zastosowanie: w transporcie lądowym, a także w portach wodnych.

Model EX80 wyposażono w dwa przetworniki CCD 480 TVL i technologię IR Black Diamond. Kamera pracuje w trybie czarno-białym i kolorowym. Detekcja z odległości do 60 m. Typowe zastosowania to: ochrona osiedli mieszkalnych, monitoring miast i szkół.

EX85 to megapikselowa kamera dualna IR z przetwornikiem 3.1 MP do pracy w dzień i 1.3 do pracy w nocy oraz z technologią IR Black Diamond. Detekcja w nocy z odległości do 128 m. Model wyróżnia odporna obudowa IP67, dlatego nadaje się on do nadzoru pomieszczeń specjalnego przeznaczenia i obronnych.

Kamera do montażu narożnego EX36 zapewnia pełną widoczność pomieszczeń do 5x5 m i umożliwia obserwację strefy podejścia pod kątem 45°. Urządzenie nie zawiera uchwytu, jest odporne na sabotaż i wandalizm. Najlepiej nadaje się do monitoringu wizyjnego więzień, aresztów, wind, szpitali.

Modele EX10 i EX14 nadają się do pracy w warunkach ekstremalnych w temperaturze od -60°C do +60°C, są wodoodporne o klasie szczelności IP67, NEMA6, NEMA6P. Model EX14, wyposażony w oświetlacz podczerwieni, umożliwia zasięg detekcji w nocy do 12 m. Kamery EX10 i EX14 nadają się do stosowania w chłodniach przemysłowych, przetwórniach spożywczych, na morzu oraz w niskiej temperaturze.

Kamera EX72 wyróżnia się obudową z ochroną przeciwpłomieniową oraz antywybuchową do zastosowań w zakładach petrochemicznych, przemyśle chemicznym czy otoczeniu kopalni.

Rodzinę kamer **MIC1** o wdzięcznym przydomku Metal Mickey wyróżnia niezwykle wytrzymała konstrukcja. Dzięki specjalnej obudowie posiadają one właściwości kwasoodporne. W ofercie jest również wersja antywybuchowa do zastosowań w kopalniach, gazowniach, cementowniach oraz modele wyjątkowo wytrzymałe na wysoką temperaturę dla straży pożarnej, jednostek ochrony granicznej i ratownictwa. Sprzęt jest odporny nawet na strzały z broni palnej. Wytrzymałość kamer MIC1-400 znacznie przewyższa właściwości dotychczas stosowanego sprzętu; są to jedyne tego typu urządzenia dostępne na polskim rynku.

Veracomp oferuje również **kamery do rozpoznawania tablic rejestracyjnych** w systemie REG. **Model REG-L1** jest w stanie zarejestrować numery pojazdów jadących z prędkością do 160 km/h w dowolnych warunkach oświetlenia i atmosferycznych. Typowe zastosowania to: płatne parkingi, budynki rządowe, obiekty handlowe, osiedla, porty, lotniska.

Grupa Bosch wzbogaciła swoją ofertę o nowe rozwiązania do monitoringu wizyjnego na skutek przejęcia Extreme CCTV. Kanadyjska firma to wiodący pod względem technologii producent i dostawca aktywnych oświetlaczy pracujących w podczerwieni, zintegrowanych kamer dualnych z aktywnym oświetleniem w podczerwieni oraz urządzeń wizyjnych o podwyższonej trwałości do zastosowań w warunkach ekstremalnych.

Bezpośr. inf. Veracomp

Najlepsze rozwiązanie w zakresie **bezpieczeństwa w handlu**

Kompleks handlowy Douglas Court w Cork w Irlandii został uznany za najlepiej strzeżony obiekt podczas gali Europejskich Rozwiązań Handlowych w Londynie. Nagrodzona instalacja, składająca się z 67 kamer sieciowych **Axis Communications** oraz oprogramowania **Milestone Systems**, zapewnia nie tylko bezpieczeństwo – jest też narzędziem do poprawy efektywności działalności handlowej.

Innowacyjny system nadzoru, bazujący na **67 kamerach sieciowych Axis**, zapewnia nie tylko bezpieczeństwo, pozwala także wyeliminować przestępstwa na terenie centrum handlowego, zmniejszyć kolejki w godzinach największego natężenia ruchu oraz zapewnić prawidłową obsługę. Kamery na bazie IP (*Internet Protocol*) pozwalają wykrywać podejrzane zachowania klientów lub pracowników, a tym samym redukują konieczność interwencji ze strony personelu i potrzebę zatrudniania osób, których zadaniem jest obserwowanie kupujących.

Po około 20 minutach patrzenia w monitor uwaga i czujność obserwatora drastycznie spadają, natomiast „inteligentna" kamera sama wykrywa podejrzane zachowania i alarmuje o nich. Integracja wideonadzoru z elektronicznymi systemami przeciwkradzieżowymi (EAS – *Electronic Article Surveillance*) pozwala zatrzymywać w bramkach klientów, którzy aktywują alarm przy drzwiach. Natomiast bezpośrednie połączenie wideo z terminalami kasowymi (POS – *Points of Sales*) umożliwia namierzenie pracowników niewłaściwie prowadzących sprzedaż (duże upusty, sprzedaż zakazanych produktów nieletnim).

– *Instalacja Axis, Milestone i RPC w centrum handlowym Douglas Court to dowód na to, jak nowoczesne systemy nadzoru nie tylko przyczyniają się do wzrostu bezpieczeństwa w sklepach, ale i stają się istotnym elementem strategii wielu firm. Nowoczesny system monitoringu to inwestycja, która przynosi po prostu wymierne korzyści biznesowe i w dłuższej perspektywie znaczące oszczędności. Przyznana nam nagroda tylko potwierdza słuszność zaangażowania w rozwiązania dla sektora handlowego* – powiedział Johan Åkesson, Business Development Director w Axis Communications.

Nowoczesne kamery sieciowe Axis pozwalają monitorować liczbę klientów wchodzących i wychodzących oraz długość kolejek przy kasie, sygnalizują braki towarów na półkach, rozlanie płynów czy zablokowanie przejść. Umożliwiają też badanie i poprawę projektu sklepu. Obserwacja zachowań i przemieszczania się kupujących umożliwia optymalizację rozmieszczenia towarów w sklepach, lepsze wykorzystanie przestrzeni handlowej, a także skierowanie dodatkowej obsługi do miejsc, w których w danym momencie znajduje się najwięcej klientów. Nagrania z kamer mogą być także narzędziem szkoleniowym dla pracowników – ich analiza uczy rozpoznawania zachowań charakterystycznych dla kradzieży sklepowych, jak i udzielania skutecznej pomocy klientom.

We wnętrzach Douglas Court zainstalowano kamery zarówno kopułkowe, jak i wyposażone w funkcje PTZ (pan/tilt/zoom) z opcją natychmiastowego pozycjonowania w pionie i poziomie oraz możliwością przybliżania. Kamery zostały zamontowane na parkingach, w 59 butikach oraz przy wejściu do centrum. Zastosowanie **systemu wideo nadzoru Milestone XProtect Enterprise** pozwala bez problemu archiwizować i przeszukiwać całodzienne nagrania, co jest szczególnie ważne w razie konieczności wyjaśnienia reklamacji czy skarg ze strony klientów. Ponadto wysokiej jakości obraz dostarczany przez kamery pozwala policji identyfikować zdarzenia mające miejsce w otoczeniu centrum handlowego.

Bezpośr. inf. Kamila Wierzbicka
Mmd Corporate Public Affairs
& Public Relations Consultants Poland

AXIS® COMMUNICATIONS

Linie lotnicze Iberia zwiększają bezpieczeństwo swoich obiektów dzięki rozwiązaniom Agent Vi

Jako największa grupa transportu powietrznego w Hiszpanii linie lotnicze Iberia (Iberia Airlines) w następstwie zamachów bombowych z 2006 roku i w celu zapobiegania kradzieżom w swoich liczących 200 000 metrów kwadratowych powierzchni obiektach zainteresowały się polepszeniem bezpieczeństwa terenów przeznaczonych wyłącznie dla samolotów. Przedsiębiorstwo to nie było zadowolone z istniejących systemów telewizji dozorowej. Aby unowocześnić swój system bezpieczeństwa, zwróciło się do amerykańskiej firmy Agent Vi – twórcy oprogramowania do analizy wizyjnej.

– *W świetle ostatnich szeroko nagłośnionych ataków i przypadków naruszenia bezpieczeństwa w licznych portach lotniczych bezpieczeństwo pozostaje naczelną troską naszego działania. Przejście do rozwiązań IP wymagało wysoce skalowalnego systemu analizy wizyjnej, który umożliwiłby nam rozmieszczenie setek kamer przy eliminacji potrzeby użycia dodatkowego sprzętu i obniżeniu kosztów operacyjnych. Oprogramowanie z firmy Agent Vi pozwoliło nam to wszystko uzyskać, a analiza wizyjna spisała się ekstremalnie dobrze, mimo stanowiącego wyzwanie środowiska zewnętrznego w pobliżu obciążonego portu lotniczego* – stwierdziła Diana Simon, szef ds. bezpieczeństwa w Iberia Airlines.

Obiekt Iberii, położony koło międzynarodowego portu lotniczego Madrid-Barajas, obejmuje siedem hangarów i komputerowe centrum operacyjne, które kontroluje odprawy, przemieszczanie się pasażerów na pokład samolotów i procesy związane z rezerwacją. Pomimo ruchu samolotów i ciężarówek po płycie lotniska, a także cieni pobliskich drzew, firma Agent Vi zapewniła Iberii łatwy sposób na dokładne wykrywanie obiektów poruszających się w zdefiniowanym obszarze, wkraczających na tereny zamknięte lub opuszczających je oraz przekraczających wirtualne linie, poprzez śledzenie zarówno kierunku, jak i prędkości tych obiektów, a także rozróżnianie ich pod względem wielkości i innych parametrów. Współpracujące z systemem Agent Vi kamery dozorowe stały się aktywnymi oczami, które automatycznie raportowały różne zachowania stanowiące przedmiot zainteresowania w czasie rzeczywistym i z ekstremalną dokładnością, twierdzi Agent Vi.

Firma Agent Vi współpracowała z lokalnym integratorem, Nordes Prosegur Tecnologia, i zainstalowała swoje oprogramowanie do analizy wizyjnej na rejestratorach sieciowych (NVR – *network video recorders*), dostarczonych przez partnera technologicznego On-Net Surveillance Systems Inc. (OnSSI).

– *Z uwagi na to, że Iberia dokonała przejścia z ograniczonego analogowego systemu CCTV do pełnego rozwiązania IP, analiza wizyjna stała się punktem krytycznym całego przedsięwzięcia, a ze względu na unikatową architekturę Agent Vi sprawdziła się jako optymalne i efektywne pod względem kosztów rozwiązanie w tym przypadku* – powiedział Javier Zammaron, szef Nordes-Prosegur.

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

Kamera **AXIS 233D**

wyposażona w funkcję automatycznego śledzenia obiektów

Firma Axis Communications wyposażyła jedną ze swoich najlepszych kamer – **AXIS 233D** Network Dome Camera – w funkcję **automatycznego śledzenia obiektów** (*auto-tracking*). Jej zastosowanie pozwala na automatyczne wykrycie poruszającej się osoby lub pojazdu i śledzenie ich ruchu w obrębie monitorowanego obszaru. Funkcja automatycznego śledzenia znajduje szczególne zastosowanie w **bezobsługowym monitoringu wideo**, zwłaszcza w sytuacji, gdy przypadkowe pojawienie się osoby lub pojazdu wymaga zwrócenia specjalnej uwagi na poruszający się obiekt.

Tradycyjny bezobsługowy monitoring wideo z funkcją automatycznego nagrywania jest najczęściej stosowany w miejscach o niewielkim natężeniu ruchu, takich jak szkoły, biura po godzinach pracy oraz sklepy, korytarze hotelowe i podziemne garaże w godzinach nocnych. Prawdziwe wyzwanie stanowi jednak uzyskanie takich funkcji, które w razie wypadku pozwolą na zarejestrowanie obrazu z interesującego nas obszaru, o jakości pozwalającej na identyfikację osoby lub pojazdu. Koszty są bardzo często tym czynnikiem, który nie pozwala na instalację dużej liczby kamer lub na zatrudnienie operatora obsługującego kamerę uchylno-obrotową. Dzięki rozszerzeniu dotychczasowych możliwości szybkoobrotowej **kamery PTZ** o funkcję automatycznego podążania za obiektem Axis wychodzi naprzeciw oczekiwaniom swoich klientów i oferuje idealne rozwiązanie tego problemu.

– Funkcja automatycznego śledzenia Axis pozwala pojedynczej kamerze szybkoobrotowej PTZ na objęcie swoim zasięgiem dużego obszaru oraz na automatyczne wykrycie, śledzenie oraz nagranie ruchu osoby lub pojazdu – mówi **Kent Fransson**, Product Manager w **Axis Communications**. *– W przypadku korzystania z bezobsługowego monitoringu **funkcja automatycznego śledzenia** umożliwia nie tylko **obniżenie kosztów** wynikające z zapotrzebowania na mniejszą liczbę kamer na danym obszarze, ale także **zwiększa efektywność** samego rozwiązania.*

Wyposażenie Axis 233D w funkcję automatycznego śledzenia pozwoliło na uzyskanie **skalowalności i elastyczności** niemożliwej do osiągnięcia w przypadku tradycyjnych kamer analogowych. Dodanie tej inteligentnej, innowacyjnej funkcji jest doskonałym odzwierciedleniem strategii Axis Communications polegającej na dążeniu do ciągłego zwiększania wartości sieciowych produktów wideo między innymi poprzez wyposażanie ich w nowe funkcje.

Obecnie sprzedawane kamery Axis 233D są standardowo wyposażane w opisywaną funkcję. Dotychczasowi użytkownicy tych urządzeń mają jednak prawo do pełnego korzystania z korzyści, jakie oferuje funkcja automatycznego śledzenia obrazu, dzięki możliwości **bezpłatnego pobrania aktualizacji wewnętrznego oprogramowania kamery** (*firmware*) ze strony producenta www.axis.com.

Źródło: www.axis.com (przekład z tekstu oryginalnego)

Dagmara Łukasiewicz, Softex Data

Nowy **czytnik kart zbliżeniowych**

Firma **Unicard** wprowadziła do sprzedaży nowy czytnik kart zbliżeniowych **ASR-802**. Czytnik jest przeznaczony do pracy w systemach kontroli dostępu. W sprzedaży dostępne są wersje czytnika współpracujące z kartami zbliżeniowymi typu **MIFARE**, **UNIQUE** lub **HITAG**. Wysoki poziom bezpieczeństwa, jaki można uzyskać stosując ASR-802, sprawia, że czytnik jest optymalnym rozwiązaniem dla firm, banków i urzędów.

ASR-802 projektowano z myślą o współpracy ze sterownikami firmy Unicard, ale dzięki wykorzystywaniu standardowych interfejsów komunikacyjnych **ABA Track II** lub **Wiegand** czytnik może współpracować ze sterownikami innych producentów. Format danych wyjściowych przekazywanych do sterownika można dostosować do indywidualnych potrzeb nabywcy.

Wielkość czytnika i nowoczesny wygląd jest odpowiedzią na potrzeby nabywców. Obudowa ASR-802 składa się z części wewnętrznej i zewnętrznej. Wszystkie elementy elektroniczne zostały zatopione w żywicy chemoutwardzalnej w obudowie wewnętrznej. Obudowa zewnętrzna pełni funkcję ozdobną i ochronną. Jest dostępna w kilku wariantach kolorystycznych, w tym malowanych farbami metalizowanymi. Obudowa zewnętrzna jest wykonana z odpornego na uderzenia tworzywa ABS. Obudowę zewnętrzną można wymieniać, nie zdejmując czytnika ze ściany.

Czytnik jest odporny na niskie temperatury i bezpośrednie działanie deszczu. Może pracować na zewnątrz. W typowych zastosowaniach czytnik jest instalowany w odległości do 30 m od sterownika. Systemy kontroli dostępu, które wykorzystują ASR-802, mogą zostać zintegrowane z innymi systemami bezpieczeństwa, np. systemami alarmowymi lub systemami przeciwpożarowymi.

Bezpośr. inf. Unicard

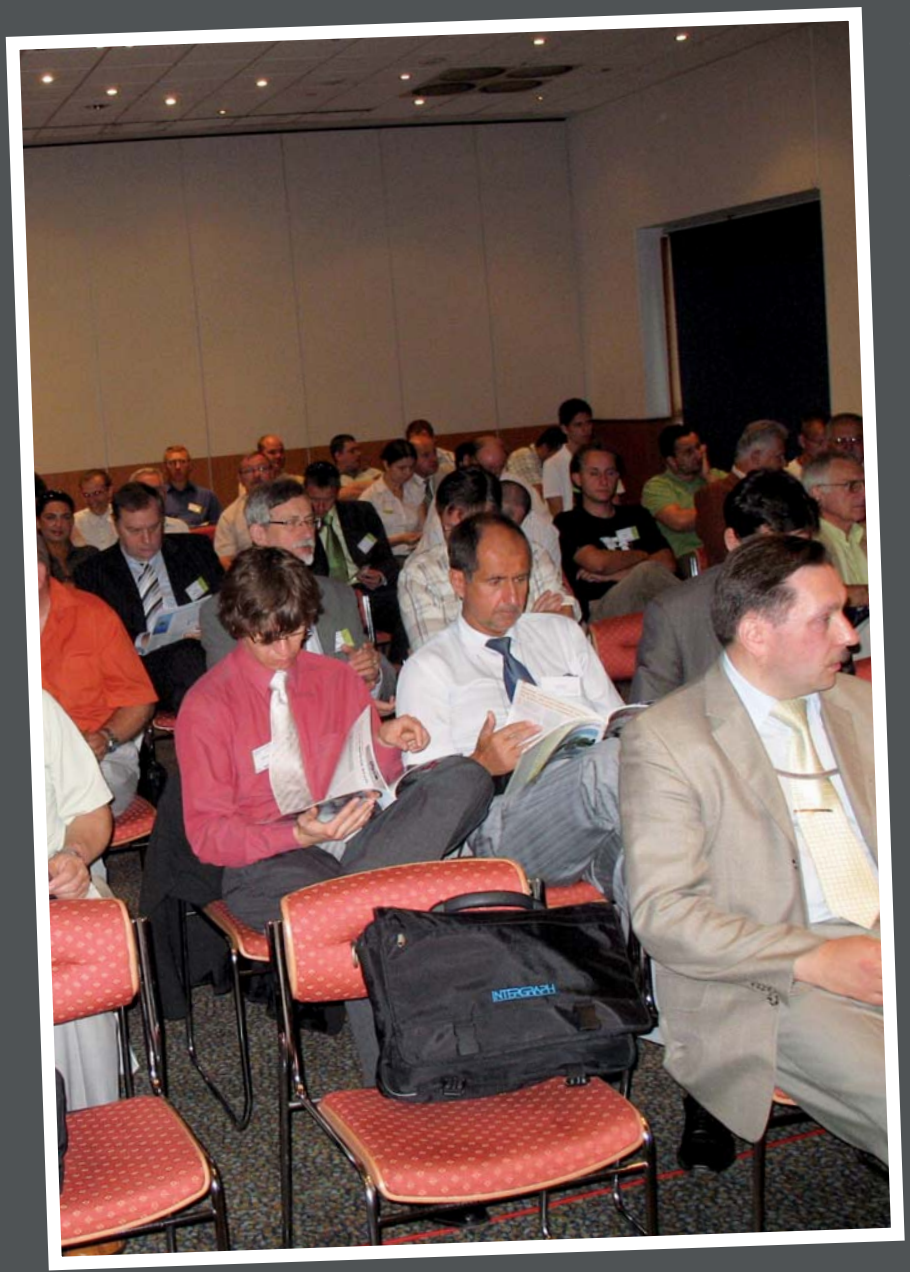
Building Security Systems GigaCon – relacja z konferencji

30 czerwca 2008 roku w hotelu Novotel Airport w Warszawie odbyła się **Konferencja Building Security Systems GigaCon**, zorganizowana przez firmę **Software Konferencje**. Konferencja była kierowana do użytkowników, instalatorów oraz projektantów systemów zabezpieczeń, osób odpowiedzialnych za bezpieczeństwo budynków, przedstawicieli firm handlowych zajmujących się sprzedażą systemów zabezpieczeń, inwestorów i deweloperów.

Sponsorem imprezy była firma **Sony**, znana na całym świecie między innymi ze swoich nowoczesnych rozwiązań do monitoringu wizyjnego. Przykłady takich rozwiązań były prezentowane na stoisku firmy Sony, gdzie od specjalistów z tej firmy oraz jej dystrybutorów można było uzyskać informacje techniczne i handlowe. Swoje stoiska miały również firmy **Fermax**, **Unicard** i Polski Komitet Normalizacyjny (**PKN**, jeden z patronów merytorycznych). Oprócz PKN patronat merytoryczny sprawowały też Polska Izba Ochrony Osób i Mienia (**PIOOiM**) oraz Wyższa Szkoła Bezpieczeństwa i Ochrony z Warszawy (**WSBiO**). Nasz dwumiesięcznik był jednym z licznych patronów medialnych.

Sponsor imprezy, patroni merytoryczni, a także firmy **AutoID** oraz **Divida** przygotowali osiem następujących referatów, z czego trzy dotyczyły systemów nadzoru wizyjnego, dwa – technologii biometrycznych, a pozostałe – problematyki ochrony osób i mienia oraz normalizacji:

1. Sławomir Wagner (PIOOiM) – „Branża ochrony osób i mienia – bezpieczeństwo obywateli”
2. Marcin Wagner (Divida) – „Problematyka zapewnienia prawidłowego funkcjonowania systemów nadzoru wizyjnego”
3. Marta Małecka (Sony) – „Monitoring wizyjny – trendy, najnowsze technologie”



4. Janusz Roszij (PKN) – „Normalizacja światowa, europejska i krajowa. Normalizacja w dziedzinie systemów alarmowych”
5. Adrian Kapczyński (Auto ID) – „Zastosowanie systemów biometrycznych w fizycznej kontroli dostępu”
6. Marta Małecka (Sony) – „Korzyści płynące z wykorzystania IP monitoringu”
7. Dobrosław Mąka (WSBiO) – „Ocena możliwości zastosowania kognitywistyki w rozwoju biometrycznych technologii kontroli dostępu”
8. Andrzej Stefański (WSBiO) –„Usługi ochrony fizycznej”

Najdonośniejszymi oklaskami zostało nagrodzone pierwsze z wystąpień Marty Małeckiej z Sony, poświęcone rozwojowi systemów monitoringu wizyjnego w ciągu ostatnich kilku lat. Zwróciła ona uwagę na postępujące w tej dziedzinie najważniejsze zmiany – prawie całkowity zanik sprzedaży kamer analogowych na rzecz kamer IP, znaczne zmniejszenie zajętości łącz sieciowych, przede wszystkim dzięki przeniesieniu inteligencji systemu do kamer IP (to w nich odbywa się współcześnie detekcja ruchu oraz przekształcanie sygnału w metadane, w wyniku czego kamera IP nie tyle transmituje obraz, co informację, a obraz tylko w niezbędnych przypadkach – tzw. wideo na żądanie) i proaktywny tryb pracy systemu informującego o zagrożeniach na podstawie informacji uzyskiwanej z kamer i podpowiadającego operatorowi, jakie czynności powinien podjąć.

Dzięki możliwości wyboru kodeków w kamerach IP trzeciej generacji można przesyłać ten sam strumień wideo z dużą kompresją (wykorzystując nowy, wydajniejszy niż dotychczas stosowane algorytm kompresji sygnału wizyjnego – H.264) np. do zdalnych centrów nadzoru i z mniejszą, ale zapewniającą lepszą jakość obrazu kompresją – lokalnie (obrazy w formacie JPEG w celu ich archiwizacji i poddania analizie). Opisane powyżej właściwości są dostępne w najnowszych produktach firmy Sony serii IPELA, symbolizującej trójstronną koncepcję „rzeczywistości” (przesyłanie informacji w czasie rzeczywistym), „inteligencji” (podejmowanie decyzji na podstawie zgromadzonej dużej ilości informacji) i „użyteczności” (rozwinięcie trybu pracy).

Adam Bułaciński
Redakcja

Ogólnopolskie Szkolenie Projektowe **Schrack Seconet** – relacja

W dniu 18 czerwca 2008 r. w Szkole Głównej Służby Pożarniczej w Warszawie odbyło się kolejne **Ogólnopolskie Szkolenie Projektowe** zorganizowane przez firmę **Schrack Seconet Polska**. Wzięło w nim udział ponad 250 osób z całego kraju, głównie projektanci oraz instalatorzy SSP. Szkolenie było bezpłatne, a wśród materiałów, jakie otrzymali jego uczestnicy, znalazła się elektroniczna wersja **podręcznika projektowania systemów sygnalizacji pożarowej oraz systemów przyzywowych i komunikacji**, produkowanych przez Schrack Seconet Polska, a także **wydanie specjalne pisma** *Opieka i Bezpieczeństwo*, zawierające prezentacje autoryzowanych partnerów organizatora szkolenia. Uczestnikom szkolenia zostaną wysłane stosowne certyfikaty. W programie szkolenia przewidziano wystąpienia przedstawicieli Schrack Seconet Polska oraz trzech zaproszonych gości specjalnych – ekspertów w dziedzinie bezpieczeństwa pożarowego.

Szkolenie rozpoczął, omawiając ten program, prezes zarządu Schrack Seconet Polska **Grzegorz Ćwiek**. Następnie **Krzysztof Kunecki**, podkreślając, jak ważna dla projektantów i użytkowników systemów jest wiedza na temat rozwiązań, które jeszcze nie są obecne na rynku, ale wkrótce się na nim pojawią, **omówił najnowsze urządzenia firmy Schrack Seconet**, które będą wprowadzane do sprzedaży w ciągu bieżącego oraz następnego roku. Należy do nich przede wszystkim kolejna **generacja central SSP serii C**, która wykorzystuje najnowszą platformę sprzętową B6 i obejmuje następujące modele przeznaczone do małych i średnich obiektów:

- **C1** – centralę jednopętlową,
- **C1 SUG** – centralę jw. z opcją jednostrefowego gaszenia,
- **C** – podstawową opcję obsługującą 2–4 pętli pożarowych,
- **C4** – model czteropętlowy.

W związku ze zbliżającą się imprezą EURO 2012 przewiduje się zwiększone zapotrzebowanie na centrale dedykowane do tej wielkości obiektów. Wśród innych zapowiedzianych produktów należy wymienić nowy przycisk o roboczej nazwie **MCP 545** oraz nową wersję **systemu zasysającego**. W tym samym wystąpieniu została także omówiona **faza 3 systemu Integral** (m.in. nowa koncepcja obudowy, nowy panel obsługi i nowa technika łączenia central w sieć) oraz **aktualny stan certyfikacji urządzeń** Schrack Seconet w Polsce.

Janusz Sawicki z Instytutu Techniki Budowlanej – gość specjalny – przedstawił zagadnienia dotyczące **kompatybilności urządzeń i sterowania w systemach bezpieczeństwa przeciwpożarowego** (m.in. podstawowe założenia dotyczące działania takich systemów oraz poziomy kompatybilności w stosunku do podzespołów tzw. rodzaju 1 i rodzaju 2) w powiązaniu z normą **PN-EN 54-13:2007**. Przybliżył także przepisy obowiązujące w tym zakresie oraz przewidziane do wprowadzenia w życie w najbliższym czasie, w tym rozporządzenie Ministra Infrastruktury, które będzie jesienią br. opublikowane wraz z nowym Prawem Budowlanym, a w którym znajdzie się kontrowersyjny zapis na temat doboru kabli niepalnych do instalacji przeciwpożarowych.

Przed przerwą ponownie zabrał głos Grzegorz Ćwiek, podsumowując **działalność Schrack Seconet Polska w roku 2007**. Obecnie firma tworzy swój drugi już, po poznańskim, oddział – tym razem we Wrocławiu, a stale zwiększająca się liczba autoryzowanych partnerów wynosi obecnie w całej Polsce ok. 35. To dzięki nim firma może pochwalić się wieloma imponującymi referencjami w naszym kraju. Do rekordowych należy **lotnisko w Krzesinach, gdzie liczba zintegrowanych ze sobą 75 central Schrack Seconet jest większa niż na przodującym dotychczas pod tym względem lotnisku Schwechat** pod Wiedniem. Do sukcesów Schrack Seconet należy też zdobycie przez wielosensorową czujkę **CUBUS MTD 533**, zastępującą obecnie stosowane w przeszłości czujki optyczne i temperaturowe, nagrody branżowego czasopisma wydawanego przez wydawnictwo GIT w kategorii ochrony przeciwpożarowej (**GIT Security Awards 2007**).

W kolejnym obszernym wystąpieniu Krzysztof Kunecki zapoznał zebranych z aktualnymi wytycznymi projektowania, konfiguracji i doboru elementów systemu **Integral Evolution** w świetle obowiązujących przepisów polskich i europejskich. Dzięki zapewnieniu **pełnej redundancji systemu oraz wysokiej odporności na zakłócenia elektromagnetyczne**, a także innym rozwiązaniom, Integral Evolution umożliwia realizację nie tylko **systemu sygnalizacji pożarowej**, ale i **systemu sterowania gaszeniem**, z możliwością pracy sieciowej w dwóch wariantach:

- **BLZ Integral Evolution** – zintegrowana centrala sygnalizacji pożarowej i sterowania gaszeniem,
- **SLZ Integral Evolution** – centrala sterowania gaszeniem dla wielostrefowego (do 32 stref) sterowania SUG (stałych urządzeń gaśniczych).

Po przerwie wystąpił drugi gość specjalny – **Jerzy Ciszewski**, także z Instytutu Techniki Budowlanej. Omówił on wybrane **wytyczne**, nie zawsze uwzględniane w należyty sposób podczas wykonywania **projektów instalacji systemów bezpieczeństwa przeciwpożarowego**. Istotnym problemem są np. **spadki napięć w instalacji przeciwpożarowej w warunkach wystąpienia pożaru**, które można obliczać w różny sposób, mniej lub bardziej dokładny, ale w każdym przypadku obliczenia powinny być wykonywane, a ich wyniki uwzględniane w projektach. W przeciwnym przypadku może okazać się, że np. poziom dźwięku DSO (dźwiękowego systemu ostrzegawczego) jest podczas pożaru dużo niższy niż zakładano i system ten nie spełnia swojego zadania prawidłowo. Autor tego wystąpienia wskazał także na **możliwości, jakie dają systemy wizualizacji (SW) lub integrujące (SI)**, nie objęte wymaganiami normy europejskiej EN 54, zwracając przy tym uwagę na **konieczność przebadania takich systemów w konkretnej konfiguracji przez upoważnione instytucje** (w Polsce: CNBOP lub ITB) **w przypadku, gdyby za ich pomocą miała być realizowana częściowa obsługa centrali sygnalizacji pożaru**, co w pewnych przypadkach jest przez tę normę dopuszczone.

Kolejny gość specjalny – **Marek Podgórski** ze Stowarzyszenia Inżynierów i Techników Pożarnictwa – poruszył rzadko prezentowany temat **zabezpieczeń stosowanych w strefach zagrożonych wybuchem** (EX). W obszernym wykładzie omówił pojęcia podstawowe obowiązujące w tej dziedzinie, w tym zasady klasyfikacji stref zagrożonych wybuchem dla palnych gazów i par cieczy, przykłady arkuszy i kart klasyfikacyjnych oraz sposób oznakowania urządzeń i systemów ochronnych, pokazał metody zabezpieczania przeciwpożarowego takich stref i podał wiele źródeł, z których te metody wynikają (normy, rozporządzenia ministerialne i dyrektywy unijne).

Z tematyką tego wykładu związane było wystąpienie **Pawła Tomaszewskiego** na temat zasad doboru urządzeń Schrack Seconet do pracy w strefach zagrożonych wybuchem oraz wytycznych ich stosowania w obiektach różnego przeznaczenia. Centrala Integral Evolution umożliwia realizację **ochrony stref zagrożonych wybuchem zarówno w technice analogowej, jak i pętlowej**, przy wykorzystaniu dedykowanych urządzeń podłączanych do centrali **bezpośrednio, przez moduł linii bocznej, barierę Zenera albo moduły lub interfejsy specjalizowane**, zależnie od rodzaju urządzenia. Dostępne są **czujki płomieni, liniowe czujki dymu, ręczne ostrzegacze pożarowe, sygnalizatory optyczne i syreny**. Podsumowaniem wystąpienia było przedstawienie ogólnych warunków stosowania czujek i ręcznych ostrzegaczy pożarowych w strefach EX.

Szkolenie zakończył Grzegorz Ćwiek, zachęcając wszystkich zainteresowanych do bezpośrednich kontaktów z zespołem Schrack Seconet Polska i zapowiadając zamieszczenie wygłoszonych podczas szkolenia prezentacji na stronach internetowych firmy.

Adam Bułaciński
Redakcja

W związku z dynamicznym rozwojem
CBC Poland Sp. z o.o.
poszukuje osób na stanowisko:

Inżynier Sprzedaży
(woj. mazowieckie)

Inżynier Sprzedaży
(woj. dolnośląskie, opolskie, śląskie, małopolskie, podkarpackie)

Zakres obowiązków:

- Aktywne prowadzenie działań sprzedażowych i marketingowych na podległym terenie
- Przygotowywanie ofert dla klientów
- Przygotowywanie raportów z wykonywanych działań
- Prowadzenie szkoleń i prezentacji u klienta
- Doradztwo w doborze sprzętu i wsparcie techniczne

Od kandydatów oczekujemy:

- Wykształcenia średniego/wyższego technicznego
- Znajomości j. angielskiego
- Prawa jazdy kategorii B
- Umiejętności interpersonalnych
- Komunikatywności
- Samodzielności
- Umiejętności rozwiązywania problemów
- Znajomość branży CCTV będzie dodatkowym atutem

Oferujemy:

- Pracę w młodym i dynamicznym zespole
- Zatrudnienie w stabilnej firmie
- Możliwość doskonalenia zawodowego

Kontakt:

Aplikacje prosimy przesyłać na adres:
praca@cbcpoland.pl

GANZ

CBC GROUP

computar

ZSJZ

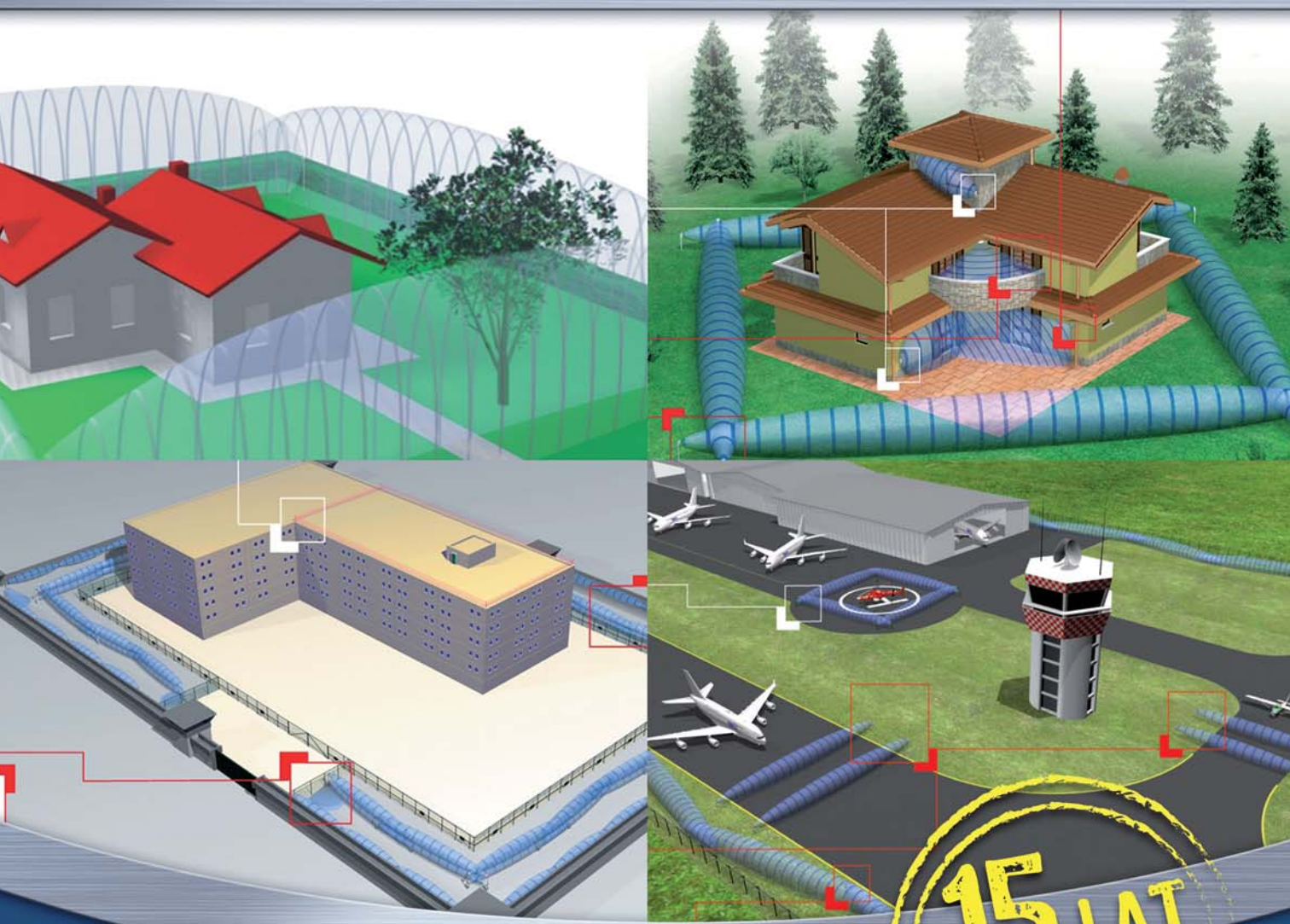
AQAP 2110:2003

SYSTEM ZARZĄDZANIA PCBC

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

firma **ATLine®**

kompleksowe zabezpieczanie obiektów



15 LAT DOŚWIADCZENIA

KOMPLEKSOWE ZABEZPIECZANIE OBIEKTÓW

15 lat doświadczenia, profesjonalizm i wysoka jakość oferowanych przez nas usług, gwarantują Państwu pełną satysfakcję.
Oferujemy Państwu atrakcyjne ceny, bezpłatne szkolenia i wsparcie fachowców w ramach zakupu.
Zapraszamy na naszą stronę www.atline.pl
Wszelkie wyceny i propozycje zabezpieczeń przeprowadzamy bezpłatnie.

- projektowanie kompleksowych dokumentacji
- wykonywanie zaawansowanych systemów bezpieczeństwa
- sprzedaż (głównie zewnętrznych systemów ochrony obwodowej)

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**

Wywiad

z Grzegorzem Tratkiewiczem, wiceprezesem spółki GEO-KAT

rozmawia Teresa Karczmarzyk

Firma GEO-KAT jest znanym na polskim rynku branżowym biurem projektowym, opracowującym rozwiązania techniczne według indywidualnych potrzeb klientów w zakresie systemów niskoprądowych. Od 10 lat realizuje projekty zarówno dla dużych, jak i mniejszych inwestorów z rynku developerskiego i przemysłu paliwowego. Firma GEO-KAT niniejszym wywiadem z wiceprezesem spółki Grzegorzem Tratkiewiczem prezentuje obraz prężnego rozwoju, wypracowanych wielu nowatorskich rozwiązań technicznych, jak i sprecyzowanych dalszych planów działania.

Proszę powiedzieć, jakie były początki Państwa działalności?

Spółka powstała na drodze połączenia dwóch specjalistycznych przedsiębiorstw, prowadzących działalność branżową od ponad dziesięciu lat. Pod nazwą GEO-KAT firma rozpoczęła swoją działalność w styczniu 2003 roku, początkowo skupiając się na projektowaniu systemów teletechnicznych.

Obecnie spółka posiada dwa niezależne działy, tj. Dział Elektronicznych Systemów Zabezpieczeń, Systemów Przeciwpożarowych i Automatyki Budynkowej BMS oraz Dział Ochrony Środowiska (zajmujący się geologią, hydrogeologią oraz rekultywacją środowiska gruntowo-wodnego). W sierpniu 2006 roku w firmie GEO-KAT został wdrożony Zintegrowany System Zarządzania Jakością ISO 9001 i 14001.

Zakres działania firmy jest bardzo szeroki. Jako biuro projektowe dysponujące własnym zapleczem sprzętowym wykonujemy projekty techniczne wykonawcze ipowykonawcze, tworzymy koncepcje projektowe oraz specyfikacje techniczne. Ponadto programujemy i uruchamiamy systemy teletechniczne w obiektach, przeprowadzamy audyty i ekspertyzy rzeczoznawcze z zakresu bezpieczeństwa, jak również zarządzamy projektami (jest to tzw. *Project Management*) metodą FIDIC i Prince2.

Należy także podkreślić, iż, wychodząc naprzeciw zapotrzebowaniom wojska i policji, utworzyliśmy w GEO-KAT Pion Informacji Niejawnych. Dysponując własną Tajną Kancelarią, jesteśmy w stanie zapewnić naszym Klientom właściwą realizację zadań zgodnie z Ustawą o Ochronie Informacji Niejawnych.

Czy specjalizujecie się Państwo w zaawansowanych i skomplikowanych technicznie projektach?

Tak, cenimy i lubimy zaawansowane i trudne przedsięwzięcia, gdzie poziom skomplikowania danego obiektu, jak i budowy całego systemu jest na tyle wysoki, że nasi specjaliści muszą budować własne, autorskie koncepcje i rozwiązania techniczne, które później są wprowadzane w obiekcie. Do projektów technicznie zaawansowanych, złożonych i długoterminowych tworzymy Zespoły Zadaniowe, które są zaangażowane tylko i wyłącznie do ich realizacji. Wielokrotnie przekonaliśmy się, że takie specjalistyczne podejście do zagadnienia jest bardziej efektywne. Mam tu na myśli terminowość prac, poprawność funkcjonowania wykonanych instalacji, jak i szeroką zdobytą wiedzę i uznanie inwestorów. Należy tutaj zauważyć, że każda inwestycja jest inna i niesie ze sobą niespodziewane sytuacje. Jeżeli chodzi o obiekty wielkokubaturowe, to nie można ich porównywać pod kątem skomplikowania i funkcjonalności – każdy jest inny.

Do opracowywania koncepcji tak skomplikowanych zagadnień zatrudniacie Państwo zapewne znakomitych specjalistów i projektantów?

Myślę, że możemy się pochwalić wykwalifikowaną kadrą projektantów, specjalistów i kierowników projektów, którzy przez ciągłe szkolenia oraz kursy stale podnoszą swe kwalifikacje oraz uzyskują uprawnienia/licencje, co procentuje podczas wykonywanych prac. Owe nieustanne podnoszenie kwalifikacji zawodowych naszej kadry potwierdza naszą rzetelność i profesjonalne podejście w zakresie świadczenia usług. Nasze uczestnictwo na rynku w wielu dużych i prestiżowych projektach pozwoliło również podkreślić rangę i kwalifikacje naszej kadry oraz dopracować metody

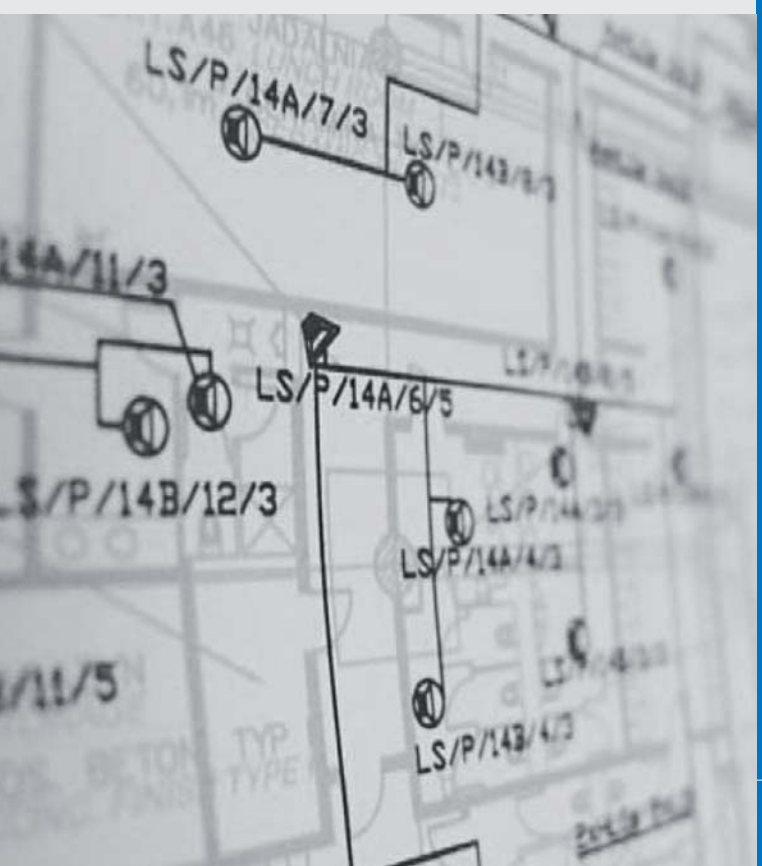
zarządzania projektami. Spółka posiada inżynierów legitymujących się co najmniej kilkuletnią praktyką zawodową. Zatrudniony zespół specjalistów nadzorujących prace pozwala nam szybko dostosować się do wymagań rynku, a zdobyte doświadczenie, potencjał projektowy oraz wypracowana pozycja na rynku polskim gwarantują solidną współpracę i stwarzają odpowiednie warunki do rozwoju firmy.

Jaki widzi Pan kierunek rozwoju firmy, obserwując obecne tendencje na rynku?

Z naszych obserwacji, rozpoznania rynku branży budowlanej, jak również wielu zapytań ofertowych od różnego rodzaju klientów wynika, iż mamy do czynienia z tendencją wzrostową jeśli chodzi o kompleksowe, wykonywane na bardzo wysokim poziomie jakościowym świadczenie usług, począwszy od tworzenia projektów, a kończąc na przekazaniu gotowych systemów końcowemu użytkownikowi, mówiąc kolokwialnie wykonawstwo „pod klucz".

Wychodząc naprzeciw tym wymaganiom, obecnie przygotowujemy się do rozszerzenia zakresu działalności o zarządzanie inwestycjami z zakresu *Construction Management*, w czym zawierać się będzie oprócz PM, czyli zarządzania projektami i QS, czyli zarządzania kosztami (od angielskiego *Quantity Surveyor* – przyp. Red.) m.in. działalność działu wykonawczo-instalacyjnego realizującego instalacje zaprojektowane przez nasz dział projektowy. Wymaga to wielu przygotowań procedur realizacyjnych z jednoczesnym pozyskaniem wykwalifikowanych kierowników robót, inspektorów nadzoru oraz specjalistów z zakresu BHP z wymaganymi uprawnieniami.

Reasumując, w Polsce istnieje jeszcze tendencja, że nie jakość a cena jest najważniejsza, ale należy zadać sobie pytanie: czy aby za wszelką cenę? Mamy nadzieję, że tę tendencję uda nam się w jakimś stopniu zmienić, gdyż właśnie dzięki jakości wykonanych usług i zastosowaniu innowacyjnych rozwiązań w późniejszej fazie możemy mówić o oszczędnościach. Wielu klientów już się o tym przekonało.



Wchodzicie w nowe płaszczyzny rynku, współpracując z pracowniami architektonicznymi – czy jest to kierunek poszukiwań nowych intratnych zleceń, któremu warto poświęcić więcej uwagi?

Nie tyle intratnych, co przede wszystkim prestiżowych. Jednym z założeń jest tutaj wykorzystywanie coraz częściej odnawialnych źródeł energii. Są to m.in. pompy ciepła, instalacje solarne itp. Mamy doświadczenie w budowie i w implementacji nowoczesnych technologii energetycznych, a przede wszystkim w budowie systemów automatyki i zarządzania budynkiem BMS zintegrowanych z tymi technologiami.

Biura architektoniczne niejednokrotnie posiłkują się naszą wiedzą i doświadczeniem w celu stworzenia najbardziej optymalnego rozwiązania technicznego do koncepcji architektoniczno-konstrukcyjnej.

Jakie projekty/inwestycje stanowią dla Państwa największe wyzwanie?

Jak wcześniej wspomniałem, największym wyzwaniem są dla nas inwestycje o dużym stopniu skomplikowania, gdzie możemy wdrażać indywidualne, autorskie, nowoczesne rozwiązania techniczne. Rozwiązania takie mają na celu ograniczenie kosztów samego wykonawstwa, ale przede wszystkim kosztów związanych z eksploatacją i konserwacją obiektów.

Czego klient może oczekiwać po GEO-KAT, powierzając wam opracowanie projektów instalacji niskoprądowych i BMS?

To, co powiem, można odnieść nie tylko do przygotowywania dokumentacji projektowych, ale również do całego zakresu prac, jakie oferujemy. Uważamy, że najważniejsze jest bezpieczeństwo i przysłowiowy „święty spokój". To właśnie gwarantujemy naszym klientom, którzy zdecydują się na skorzystanie z naszych usług. Poprzez wypracowanie własnych metod prowadzenia inwestycji zapewniamy bezpieczeństwo i sukces w realizacji powierzonych nam zadań, a poprzez podejście, zaangażowanie i profesjonalizm – „święty spokój", czyli brak problemów naszych klientów w bezpośredniej styczności z wykonawcami, generalnym wykonawcą czy samym inwestorem.

Reasumując, należy zauważyć, że nasze portfolio i lista prestiżowych przedsięwzięć, przy których realizacji uczestniczyliśmy bądź odgrywaliśmy kluczową rolę, stanowią tylko potwierdzenie moich słów.

PHISHING

polowanie na łatwowiernych

(część I)

Większość nowinek technicznych ułatwia funkcjonowanie w otaczającej nas rzeczywistości. Codzienne czynności stają się łatwiejsze, więcej spraw możemy załatwić w krótszym czasie, a coraz więcej z nich bez potrzeby wychodzenia z domu czy przerywania pracy przy komputerze. Prawdziwe oblężenie przeżywają internetowe portale aukcyjne. Ich rozwój w ostatnich latach powoduje, iż biją one kolejne rekordy w obrotach finansowych. Z kolei możliwość realizacji operacji bankowych dzięki elektronicznemu kanałowi dostępowemu sprawia, iż zamiast marnotrawić własny czas na dojazd do oddziału banku, a później nerwowo oczekiwać na swoją kolej do kasjerskiego okienka, wolimy usiąść wygodnie przed ekranem domowego czy służbowego komputera i w dogodnej dla siebie chwili zrealizować konieczny przelew. Niestety, jak w większości przypadków tak i tutaj mamy do czynienia nie tylko z samymi plusami, jakie niosą za sobą coraz większe możliwości sieci Internet. Aby korzystać z oferowanych przez sieć usług wygodnie i bez stresu, należy znać podstawowe niebezpieczeństwa, które czyhają na użytkownika na każdym kroku. Jednym z takich bardzo popularnych niebezpieczeństw jest *phishing*[1].

Aby rozpocząć rozważania na temat problemu, jakim jest *phishing*, należy rozszyfrować znaczenie tego słowa. Geneza terminu nie jest jasna. Jedne źródła podają, iż wyraz *„phishing”* powstał w wyniku skrzyżowania słowa *„fishing”* („wędkowanie”) oraz frazy *„personal data”* („dane personalne”). Inne, że termin *„phishing”* powstał jako skrót wyrażenia *„password harvesting fishing”* („łowienie haseł”) lub że termin pochodzi od nazwiska Briana Phisha, który miał być pierwszą osobą stosującą techniki psychologiczne do wykradania numerów kart kredytowych w latach 80. Jeszcze inni uważają, że Brian Phish był jedynie fikcyjną postacią, za pomocą której spamerzy wzajemnie się rozpoznawali[2].

Zjawisko phishingu polega na tworzeniu przez oszusta sfałszowanych wiadomości e-mail i witryn WWW, które wyglądają identycznie jak serwisy internetowe firm o znanej marce, w celu skłonienia klientów indywidualnych do podania numeru karty kredytowej, informacji o koncie bankowym, hasła dostępu do niego[3]. Dlatego *phishing* uważany jest za formę kradzieży tożsamości. Należy pamiętać, iż *phishing* jest prowadzony przede wszystkim przez Internet – z wykorzystaniem spamu (rozsyłanie do dużej liczby nieznanych adresatów niechcianych wiadomości e-mail) lub różnych odmian wirusów komputerowych, ale może być prowadzony również przez telefon bądź osobiście, za pomocą różnych taktyk socjotechnicznych. Oszust zajmujący się procederem phishingu wysyła zazwyczaj odpowiednio spreparowany spam do ogromnej liczby potencjalnych ofiar, kierując je na stronę w sieci, która przechwytuje wpisywane tam przez ofiary ataku informacje. Witryny w sieci Internet, do których użytkownicy są odsyłani, wyglądają bardzo oficjalnie, do złudzenia podobnie do autentycznych, i wielu internautów bierze je za prawdziwe. Niektórzy z nich – niczego nie podejrzewając – podają numery kart kredytowych, loginy, hasła, jednorazowe kody do potwierdzania realizacji zleceń przelewów z kont internetowych lub swoje dane osobowe[4].

Przestępcy zajmujący się phishingiem stają się coraz bardziej wyrafinowani, dokładni i precyzyjni – takie też stają się fałszywe e-maile lub spreparowane strony WWW. Coraz częściej zawierają oficjalne symbole, logo rzeczywistej firmy lub organizacji oraz informacje identyfikacyjne wzięte bezpośrednio z autentycznych witryn. Gdy użytkownik znajdzie się na takiej spreparowanej stronie internetowej, może nieświadomie wysłać oszustowi swoje informacje osobiste. Oszuści następnie często wykorzystują takie dane do dokonania włamania na konto bankowe (a w konsekwencji realizacji przelewu środków zgromadzonych na takim rachunku na inne

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.)

2) http://pl.wikipedia.org/wiki/Phishing
3) http://www.symantec.com/region/pl/plresc/phishing.html
4) http://www.microsoft.com/poland/athome/security/email/phishing.mspx

konta, najczęściej założone na tzw. „słupy"), zakupu towarów, ubiegania się o nową kartę kredytową[5]. Aby nakłonić do skierowania się na spreparowaną stronę, przestępcy posługują się wirusami komputerowymi typu trojan lub przesyłają do użytkowników wiadomości e-mail z odpowiednio sformułowaną treścią.

Oto przykładowa treść wiadomości e-mail związanej z phishingiem, która pojawiła się w skrzynkach użytkowników poczty elektronicznej w 2007 roku:

„Witamy w systemie Aktualizacji Systemu(...)
Zaktualizuj swój komputer
System Aktualizacji Systemu (...) zeskanował Twój komputer i znalazł krytyczne błędy w systemie. Prosimy o jak najszybszą aktualizację systemu. Zignorowanie tej wiadomości i brak aktualizacji może spowodować całkowitą i bezpowrotną utratę danych z komputera (w celu aktualizacji kliknij w przycisk niżej «Pobierz teraz i zainstaluj»)."

W przypadku kliknięcia odnośnika zawartego w tej wiadomości na komputer ofiary ataku zostawał „załadowany" automatycznie wirus typu trojan, który wykradał wpisywane przez użytkownika za pośrednictwem klawiatury poufne dane i przesyłał je na serwer opanowany przez przestępców. W tym przypadku mamy do czynienia z atakiem na użytkowników konkretnego systemu operacyjnego, ale podobna sytuacja występuje również, gdy atak dotyczy użytkowników posiadających uprawnienia do realizacji elektronicznych operacji na kontach bankowych, przy realizacji płatności w Internecie z wykorzystaniem kart płatniczych lub w przypadku posiadania uprawnień dostępu do innych usług internetowych. Aby jeszcze bardziej uwiarygodnić wiadomość e-mail, oszust może umieścić w niej łącze wyglądające na prowadzące do autentycznej witryny WWW, gdy w rzeczywistości prowadzi ono do sfałszowanej strony lub ewentualnie wyskakującego okna wyglądającego dokładnie tak, jak autentyczna witryna.

Treść spreparowanych wiadomości najczęściej jednak posiada cechy wskazujące na to, iż są one narzędziem stworzonym przez phishera. Gdy otrzymamy podejrzaną wiadomość e-mail, należy zwrócić uwagę, czy nie zawiera ona charakterystycznych dla phishingu sformułowań.

Poniżej przedstawiono kilka z wielu sformułowań, na które należy zwracać uwagę w przypadku, gdy zachodzi podejrzenie, że wiadomość e-mail jest związana z phishingiem:

1. „Zweryfikuj swoje konto" – ogólnie przyjętą zasadą jest to, że firmy nie proszą o przesyłanie haseł, nazw użytkownika, numerów PESEL czy innych informacji osobistych pocztą e-mail. Ostrożnie należy podchodzić do wiadomości z prośbą o podanie informacji osobistych, nawet jeśli prośba taka wydaje się być uzasadniona.

2. W przypadku braku odpowiedzi w ciągu 48 godzin Pani/Pana konto zostanie zamknięte – wiadomość e-mail związana z phishingiem może być uprzejma i stonowana, jednak najczęściej ma ponaglający wydźwięk, by użytkownik bez zastanowienia się odpowiedział na nią. Treść wiadomości może zawierać ostrzeżenie o zamknięciu lub zawieszeniu konta albo nawet stwierdzać, że odpowiedź jest niezbędna ze względów bezpieczeństwa.

3. „Szanowny Kliencie" – wiadomości e-mail związane z phishingiem są zwykle rozsyłane masowo i nie zawierają imienia ani nazwiska. Większość legalnie działających firm (ale nie wszystkie) zwracają się do klientów, używając imienia i nazwiska.

4. „Kliknij poniższe łącze, aby uzyskać dostęp do swego konta" – wiadomości mogą zawierać łącza lub formularze, które można wypełniać tak, jak formularze zawarte na stronach sieci Internet. Łącza, do kliknięcia których zachęcany jest użytkownik, mogą zawierać całą nazwę rzeczywistej firmy lub jej część i są zwykle zamaskowane. Oznacza to, że łącze nie prowadzi do adresu, który jest na nim wyświetlany, lecz w inne miejsce, zwykle do fałszywej witryny w sieci[6].

Na następnej stronie prezentujemy przykłady spreparowanych listów poczty elektronicznej, których duża liczba trafia na nasze konta pocztowe.

Inną metodą powszechnie wykorzystywaną przez oszustów jest używanie adresu internetowego, który na pierwszy rzut oka wygląda jak nazwa renomowanej firmy, lecz w rzeczywistości jest nieco zmieniony poprzez celowe przestawienie, opuszczenie lub dodanie liter. Na przykład adres www.zabezpieczenia.com.pl mógłby przyjąć postać:

- www.zabepieczenia.com.pl – przestawienie liter „z" i „c",
- www.zabepieczenia.com.pl – pominięcie jednej z liter „z",
- www.gazeta-zabezpieczenia.com.pl – dodanie dodatkowego wyrażenia „gazeta-".

W drugiej części artykułu zostaną omówione różne odmiany phishingu, 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 procederu phishingu, a także sposoby zabezpieczenia się przed nim.

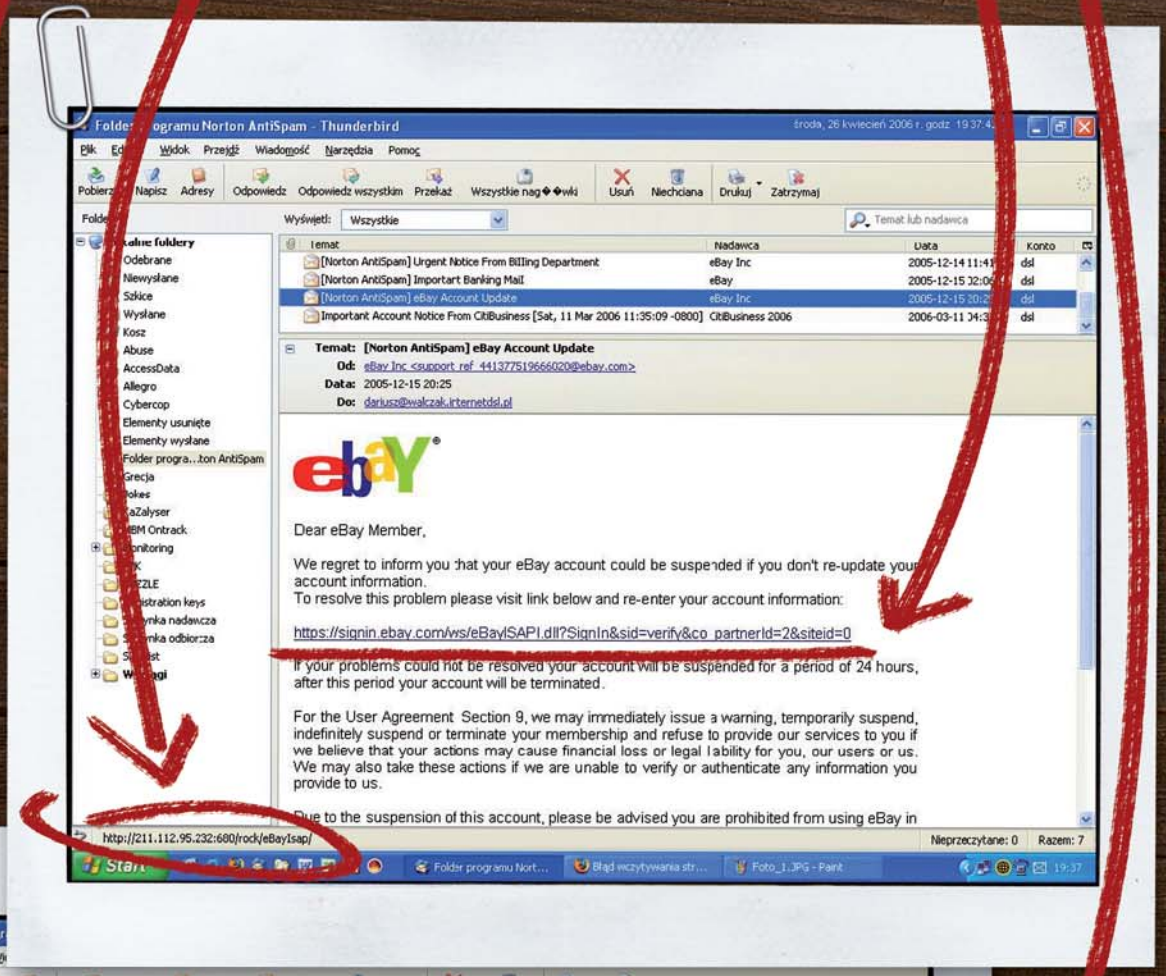
KRZYSZTOF BIAŁEK

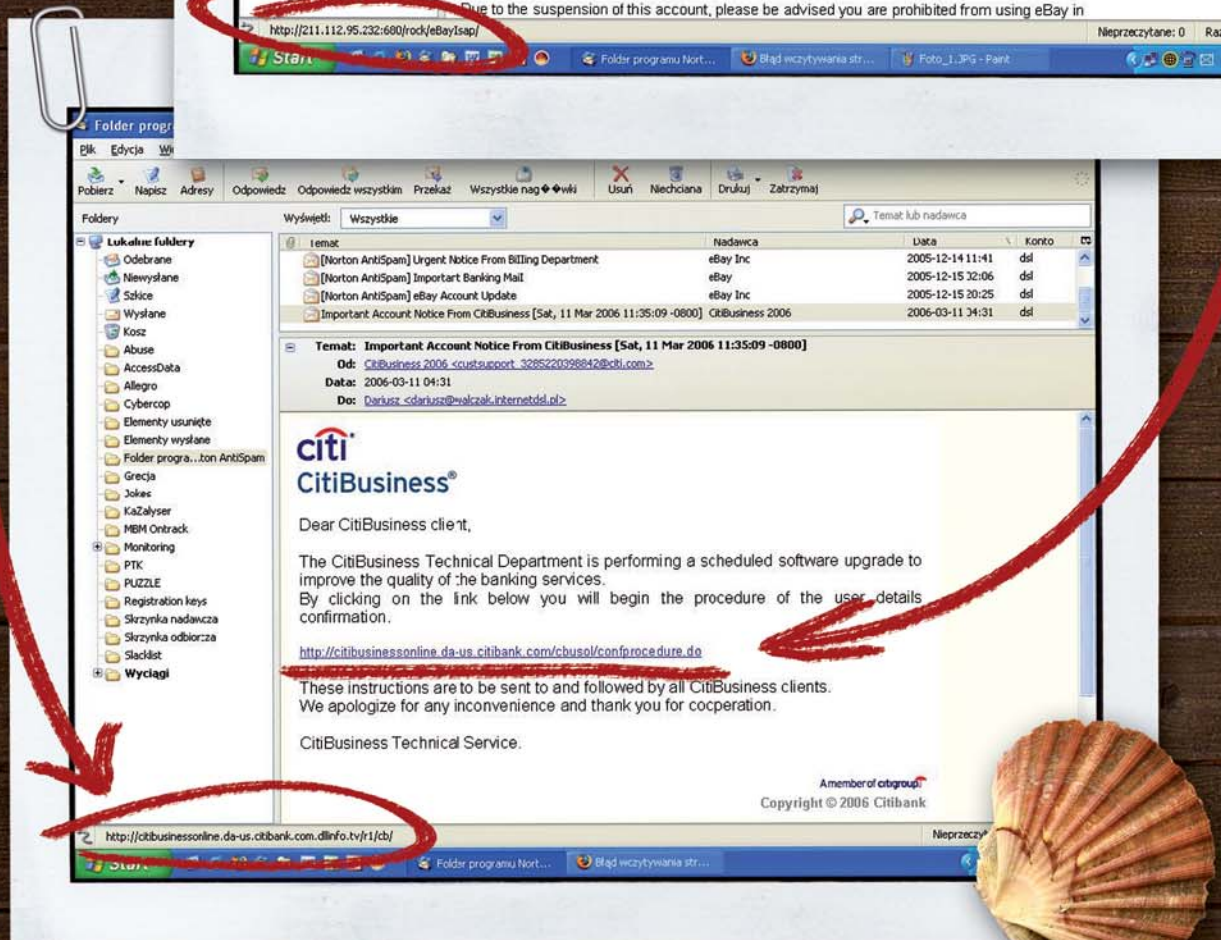
Rys. 1. Przykład zamaskowanego adresu URL. Źródło: http://www.microsoft.com/poland/athome/security/email/phishing.mspx

5) http://www.microsoft.com/poland/athome/security/email/phishing.mspx

6) http://www.microsoft.com/poland/athome/security/email/phishing.mspx

ADRES WYŚWIETLANY W TREŚCI LISTU I ADRES RZECZYWISTY





System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001

Cz. 3. Elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Artykuł ten jest kontynuacją cyklu poświęconego zarządzaniu bezpieczeństwem informacji zgodnemu z normą ISO/IEC 27001. W kolejnej części zostanie omówiony jeden z modeli zarządzania bezpieczeństwem systemów informatycznych (PDCA)

1. Wprowadzenie

ISO/IEC 27001:2005[1] jest międzynarodowym standardem dotyczącym zarządzania bezpieczeństwem informacji wydanym w 2005 r. przez ISO (*International Organization for Standardization*) i Międzynarodowy Komitet Elektrotechniczny (*International Electrotechnical Commission*), opracowanym na podstawie wycofanej już brytyjskiej normy BS7799-2:2002. Istnieją również wydane przez Polski Komitet Normalizacyjny polskie odpowiedniki obu standardów – aktualny PN-ISO/IEC 27001:2007 oraz wycofany PN-I-07799:2005. ISO/IEC 27001:2005 określa wymagania dla ustanowienia, wdrożenia, zarządzania, monitorowania i przeglądu udokumentowanego systemu zarządzania bezpieczeństwem informacji (SZBI) oraz 11 obszarów mechanizmów kontrolnych obejmujących:

- politykę bezpieczeństwa,
- organizację bezpieczeństwa,
- zarządzanie aktywami,
- bezpieczeństwo zasobów ludzkich,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,
- kontrolę dostępu,
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
- zarządzanie incydentami bezpieczeństwa,
- zarządzanie ciągłością działania,
- zapewnienie zgodności z wymaganiami wewnętrznymi i prawnymi.

Na tej podstawie należy stwierdzić, iż opisywany standard gwarantuje w pełni kompleksowe podejście do problemu bezpieczeństwa informacji, obejmując swym zakresem nie tylko zagadnienia związane z teleinformatyką, lecz również z bezpieczeństwem osobowym, fizycznym oraz organizacyjno-prawnym.

1) Na podstawie witryny *http://www.iso27000.pl/* firmy PBSG

2. Standard ISO/IEC 27001

Wg PN 1-0/799-2:2005 system zarządzania bezpieczeństwem informacji (*ISMS – Information Security Management System*)[2] to część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

ISMS dotyczy struktury organizacyjnej, polityki, zaplanowanych działań, zakresów odpowiedzialności, zasobów, procesów oraz procedur. Na proces planowania i implementacji ISMS wpływają potrzeby i cele biznesowe, wymagania bezpieczeństwa, wykonywane procesy oraz wielkość i struktura jednostki. Wdrożenie systemu zarządzania bezpieczeństwem informacji powinno być dla organizacji decyzją strategiczną.

Ustanowienie SZBI (ISMS)

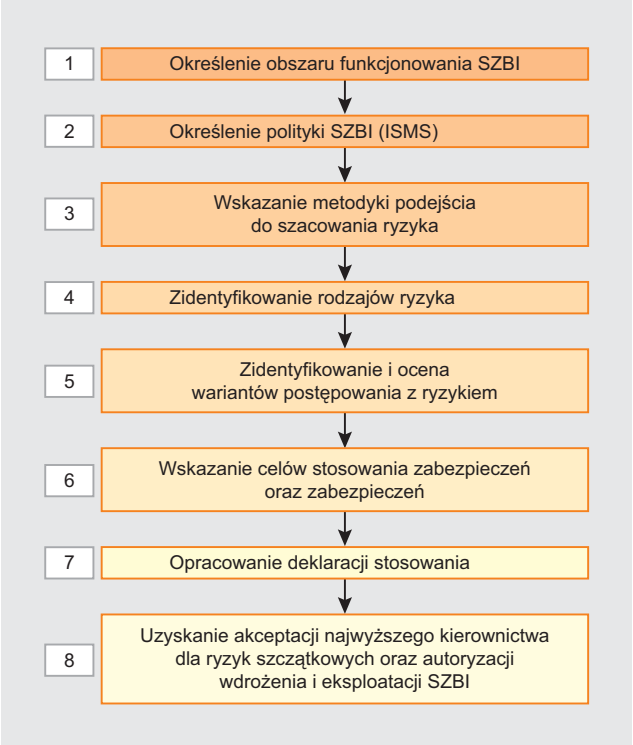
Ustanowienie efektywnie działającego ISMS wymaga systematycznego podejścia i zwykle prowadzone jest w ramach kilku etapów (rys. 1)[3] .

Zakres ISMS powinien uwzględniać charakter prowadzonej działalności, zasoby będące w posiadaniu jednostki oraz jej lokalizację i stosowane technologie.

Opracowując politykę ISMS, należy wziąć pod uwagę te

2) Zamiennie zamiast skrótu ISMS można stosować skrót SZBI. Takie podejście stosowane jest także w niniejszym artykule.

3) Na podstawie Marian Molski, Małgorzata Łacheta, *Przewodnik audytora systemów informatycznych*



Rys. 1. Etapy ustanawiania SZBI (ISMS)

same parametry, co w przypadku określania zakresu systemu. Ponadto dokument ten powinien:

- zawierać cele i zasady działania dotyczące zarządzania bezpieczeństwem informacji;
- uwzględniać wymagania biznesowe, prawne, kierownictwa i zobowiązania wynikające z umów;
- wyznaczać kontekst strategiczny oraz kontekst zarządzania ryzykiem;
- wskazywać kryteria oceny ryzyka i strukturę jego szacowania;
- być zaakceptowany przez kierownictwo.

Systematyczne podejście do szacowania ryzyka wymaga:

- wskazania odpowiedniej metody działania;
- określenia bezpieczeństwa informacji w odniesieniu do ryzyka biznesowego, wymagań prawnych i nadzoru;
- ustanowienia polityki ISMS w celu zmniejszenia ryzyk do akceptowalnego poziomu;
- wskazania kryteriów akceptowania ryzyka;
- zidentyfikowania akceptowalnych poziomów ryzyka.

Identyfikacja rodzajów ryzyka polega na:

- wskazaniu zasobów i ich gestorów będących w zakresie ISMS;
- określeniu zagrożeń dla zidentyfikowanych zasobów;
- wskazaniu podatności dla zidentyfikowanych zasobów;
- określeniu skutków materializacji zagrożenia.

Szacowanie ryzyka polega na:

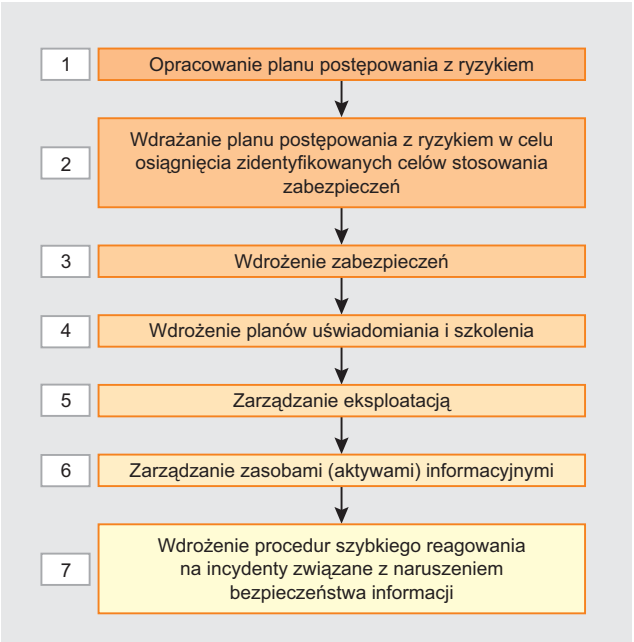
- oszacowaniu potencjalnych strat biznesowych wynikających z naruszenia bezpieczeństwa informacji;
- określeniu realnego prawdopodobieństwa wystąpienia niekorzystnych dla jednostki zdarzeń;
- wyznaczeniu poziomu zidentyfikowanych rodzajów ryzyka; określeniu, czy ryzyko jest akceptowalne.

Istnieją następujące warianty traktowania ryzyka:

– wdrożenie zabezpieczeń,
– unikanie ryzyka,
– zaakceptowanie ryzyka,
– transfer ryzyka, np. na ubezpieczycieli.

Cele stosowania zabezpieczeń i odpowiednie mechanizmy zabezpieczające można wybrać na podstawie załącznika A normy PN-I-07799-2, lecz nie jest to lista wyczerpująca i w niektórych przypadkach celowe jest również użycie zabezpieczeń dodatkowych.

W deklaracji stosowania ISMS powinny być wymienione: zabezpieczenia, uzasadnienie ich wyboru oraz udokumentowane cele stosowania zabezpieczeń.



Rys. 2. Zasady wdrażania i eksploatacji SZBI (ISMS)

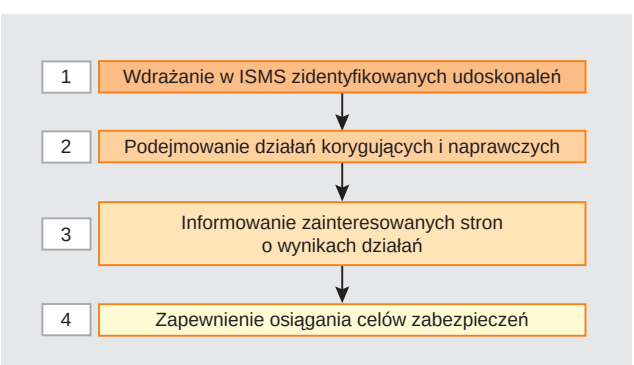
Wdrożenie i eksploatacja SZBI (ISMS)

W celu prawidłowego wdrożenia i eksploatacji ISMS organizacja powinna wykonać kilka podstawowych działań[4] (rys. 2).

Monitorowanie i przegląd SZBI (ISMS)

W ramach monitorowania i przeglądu organizacja powinna:

- wykonywać procedury szybkiego reagowania na incydenty naruszenia bezpieczeństwa informacji;
- realizować regularne przeglądy skuteczności ISMS



Rys. 3. Zasady prawidłowego utrzymania SZBI (ISMS)

4) Na podstawie Marian Molski, Małgorzata Łacheta, *Przewodnik audytora systemów informatycznych*

(zgodność z polityką i celami oraz przegląd zabezpieczeń) z wykorzystaniem wyników audytów bezpieczeństwa;
– wykonywać przeglądy poziomu ryzyka szczątkowego oraz akceptowalnego z uwzględnieniem zmian technologicznych, celów biznesowych, zagrożeń, uregulowań normatywnych i ustawowych;
– przeprowadzać wewnętrzne audyty ISMS z odpowiednio dobraną częstotliwością działań;
– wykonywać przeglądy ISMS realizowane przez kierownictwo (przynajmniej raz w roku).

Utrzymanie i doskonalenie SZBI (ISMS)

W celu skutecznego utrzymania i doskonalenia ISMS organizacja powinna wykonać kilka podstawowych działań[5] (rys. 3).

Wymagania dotyczące dokumentacji

Prawidłowo opracowana dokumentacja ISMS zawiera:
– deklaracje polityki bezpieczeństwa i celów stosowania zabezpieczeń;
– określenie zakresu ISMS oraz zabezpieczeń potrzebnych do realizacji ISMS;
– raport z procesu szacowania ryzyka;
– plan postępowania z ryzykiem;
– udokumentowane procedury niezbędne do zapewnienia efektywnego zarządzania bezpieczeństwem informacji;
– deklarację stosowania.

W zależności od wielkości organizacji, rodzaju prowadzonej działalności oraz złożoności wymagań bezpieczeństwa zakres dokumentacji ISMS będzie odmienny.

Dokumenty mogą mieć dowolną formę i mogą być przechowywane na dowolnym typie nośnika.

Zasady udostępniania dokumentacji określone są w polityce ISMS.

Przegląd realizowany przez kierownictwo

Norma PN-I-07799-2:2005 zobowiązuje kierownictwo do przeprowadzania regularnych przeglądów ISMS, mających na celu zapewnienie, że system działa poprawnie i skutecznie oraz jest adekwatny do potrzeb organizacji. Przegląd obejmuje ocenę możliwości doskonalenia i potrzeby zmian w ISMS. Wyniki przeglądu powinny być jasno udokumentowane.

Dane wejściowe i wyjściowe przeglądu

Można wskazać następujące dane wejściowe przeglądu realizowanego przez kierownictwo:
– wyniki audytów i przeglądów ISMS,
– informacje zebrane od zainteresowanych stron,
– techniki i procedury możliwe do zastosowania w organizacji w celu udoskonalenia ISMS,
– informacje na temat działań korygujących i naprawczych,
– podatności lub zagrożenia nieobjęte poprzednim oszacowaniem ryzyka,
– działania podjęte w ramach wdrażania rekomendacji z poprzednich przeglądów wykonanych przez kierownictwo,
– zmiany w zakresie ISMS,
– zalecenia dotyczące doskonalenia ISMS.

Do danych wyjściowych omawianego przeglądu należą działania i decyzje mające związek z:
– doskonaleniem ISMS,
– zmianami procedur w zakresie bezpieczeństwa informacji,
– potrzebnymi zasobami.

Wewnętrzne audyty

Wewnętrzne audyty ISMS powinny być odpowiednio zaplanowane i prowadzone regularnie. Celem działań audytowych jest weryfikacja:
– zgodności z wymaganiami normy PN-I-07799-2:2005 innymi regulacjami prawnymi i normatywnymi;
– zgodności z wymaganiami bezpieczeństwa informacji;
– efektywności wdrożenia i utrzymania systemu zarządzania bezpieczeństwem informacji;
– zgodności działania ISMS z zamierzeniami.

Program audytu powinien wskazywać kryteria, zakres, częstotliwość i przyjętą metodykę audytu.

5) Na podstawie Marian Molski, Małgorzata Łacheta, *Przewodnik audytora systemów informatycznych*

DR INŻ. ANDRZEJ WÓJCIK

ACTIVA
bariery podczerwieni

Wszechstronność zastosowań, **niezawodność i atrakcyjna stylistyka** to główne atuty barier podczerwieni **ACTIVA**, gwarantujących skuteczną ochronę obwodową wewnątrz budynku i na zewnątrz.

W skład oferty wchodzi 7 modeli barier, różniących się między sobą długością i ilością wiązek. Dostępne są w dwóch kolorach obudowy.

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

NIEBEZPIECZEŃSTWA
PŁYNĄCE Z SIECI WEWNĘTRZNEJ KORPORACJI – SPOSÓB OBRONY

Na dzisiejszym rynku, a zwłaszcza na rynku związanym z nowoczesnymi technologiami, wartość informacji jest coraz większa w stosunku do zasobów materialnych posiadanych przez firmę i trend ten stale rośnie. Szacuje się, że w roku 2007 na świecie znajdowało się około 281 EB informacji (1 eksabajt to 1024*1024*1024 GB), co daje 45 GB informacji na każdego człowieka na ziemi.

Co więcej, według raportu IDC „The Diverse and Exploding Digital Universe: An Updated Forecast of Worldwide Information Growth Through 2011" (Zróżnicowany i eksplodujący wszechświat cyfrowy: zaktualizowana prognoza wzrostu ilości informacji na świecie do roku 2011) w 2011 ilość ta wzrośnie do 1,8 ZB (1 zettabajt to 1024 eksabajtów). Pomimo tego, że połowa tych informacji jest wynikiem działań indywidualnych ludzi (takich jak zdjęcia cyfrowe itd.), przedsiębiorstwa są odpowiedzialne za bezpieczeństwo ponad 85% tych informacji. – *W miarę jak rośnie ilość śladów cyfrowych pozostawianych przez ludzi, rosnąć też będzie odpowiedzialność przedsiębiorstw i instytucji za prywatność, ochronę, dostępność oraz rzetelność tej informacji. Działy informatyczne przedsiębiorstw będą musiały stawić czoła problemom związanym z ryzykiem, zgodnością z przepisami, niewłaściwym użyciem informacji, wyciekiem danych oraz ochroną przed naruszeniami bezpieczeństwa* – powiedział Joe Tucci, przewodniczący rady nadzorczej, prezes zarządu i dyrektor generalny EMC.

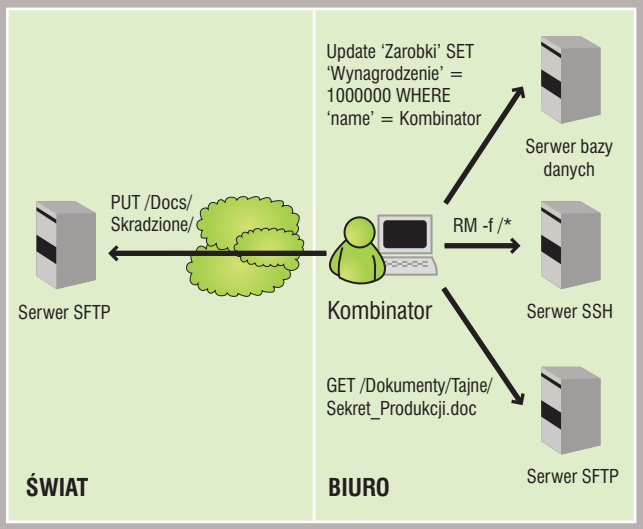
Skoro znamy już szacunki co do ilości informacji na świecie, spróbujmy zdefiniować jeszcze pojęcie wartości informacji. Istnieje wiele formalnych i nieformalnych definicji. Jedna z najpopularniejszych jest następująca: „wartość informacji jest równa cenie, jaką osoba potrzebująca takiej informacji jest skłonna zapłacić". Osobiście nie lubię tej definicji, ponieważ dla każdego dana informacja może mieć zupełnie inną wartość. Znacznie bardziej trafna wydaje mi się definicja, która mówi, że „wartość informacji jest równa sumie strat, jaką może spowodować niedostępność, utrata, kradzież lub zafałszowanie tej informacji". Straty takie można podzielić na bezpośrednie, wynikające na przykład z defraudacji lub z działalności konkurencji wykorzystującej ukradzione informacje, oraz pośrednie – takie jak na przykład utrata reputacji w wyniku przeprowadzonego ataku. Należy podkreślić, że według badań statystycznych większość zagrożeń dla informacji pochodzi z sieci wewnętrznej, co więcej nie muszą to być celowe działania. Wiele takich zagrożeń wynika z niedbałości lub niewiedzy użytkowników sieci wewnętrznej. Dlatego jednym z podstawowych celów każdej korporacji powinno być zabezpieczenie danych przed utratą, kradzieżą oraz zafałszowaniem. – *Biorąc pod uwagę, że odpowiedzialność za 85% tworzonych i kopiowanych informacji będą ponosić organizacje i przedsiębiorstwa, musimy jako branża podejmować kroki, które zapewnią nam opracowanie elastycznych, godnych zaufania i bezpiecznych infrastruktur informatycznych, które będą w stanie przetworzyć rosnącą ilość przepływających informacji* – mówi w wyżej już wspomnianym raporcie Mark Lewis, wiceprezes wykonawczy i dyrektor ds. rozwoju firmy EMC Corporation. Potrzebna nam będzie jeszcze jedna definicja, bo co to właściwie znaczy, że informacja jest bezpieczna? Jak powszechnie wiadomo, żaden system nie może być w pełni bezpieczny, zawsze istnieją jakieś luki bądź to w oprogramowaniu, bądź w procedurach, czy wreszcie po prostu błędy lub celowe działania ludzi, którzy system obsługują. Idealna definicja na potrzeby tego artykułu będzie następująca: „informację uważamy za bezpieczną, jeśli koszty poniesione na kradzież, zafałszowanie lub spowodowanie utraty są wyższe niż potencjalne zyski dla osoby próbującej taką operację przeprowadzić".

Więc jak ten cel zrealizować? Podstawą bezpieczeństwa w każdej korporacji jest dobrze zdefiniowana polityka bezpieczeństwa. Niestety w większości przypadków jest to martwy

Protokół	Zapisywane informacje
HTTP	Nagłówki żądań i odpowiedzi HTTP
FTP	Polecenia i odpowiedzi przesyłane w połączeniu kontrolnym FTP
telnet	Polecenia wykonywane przez użytkownika i odpowiedzi serwera
SSH (szyfrowany)	
POP3	Wykonane polecenia i status ich wykonania, bez zawartości odbieranej poczty. Z technologicznego punktu widzenia jest to możliwe, natomiast z przyczyn etycznych z reguły ta możliwość jest wyłączana
IMAP	
SMTP	Z technologicznego punktu widzenia jest to możliwe, natomiast z przyczyn etycznych z reguły ta możliwość jest wyłączana
SMB	Operacje wykonane na plikach lub katalogach i status ich wykonania, bez zawartości plików. Podobnie jak w przypadku protokołów pocztowych istnieje możliwość zapisywania plików, natomiast z reguły jest to wyłączone z powodu dużej ilości miejsca, jakie zajmowałyby te pliki
NFS	
Oracle	Wykonane zapytania SQL i status ich wykonania (pomyślny lub błąd) – bez danych. Podobnie jak w przypadku protokołów pocztowych istnieje możliwość zapisywania danych, natomiast z reguły jest ona wyłączona z powodu dużej ilości miejsca, jakie zajmowałyby te pliki
MySQL	
PostgreSQL	
MsSQL	
X11 (szyfrowany)	Zrzuty ekranu wykonywane w konfigurowalnych odstępach czasu. Zapis klawiszy naciskanych przez użytkownika
SSL	Daje możliwość analizowania wszystkich protokołów nieszyfrowanych, tunelowanych z wykorzystaniem SSL
Dowolny protokół	System SecureAdmin posiada API[1], za pomocą którego można stworzyć analizator dowolnego protokołu. Dzięki temu korporacje dostają możliwość monitorowania własnych zamkniętych protokołów

Tab. 1. Protokoły sieciowe obsługiwane przez SecureAdmin
[1]API – ang. Application Programming Interface – interfejs programowania aplikacji

dokument. Istnieje wiele sposobów wspomagania realizacji polityki bezpieczeństwa, takich jak szkolenia, audyty, kontrola wewnętrzna i najważniejsze ze wszystkich – narzędzia. Sama polityka bezpieczeństwa oraz metody jej wymuszania są tematem na osobny artykuł. W tym artykule spróbuję przedstawić jedno z narzędzi autorstwa firmy Comarch, którego celem jest zabezpieczenie informacji zgromadzonych w wewnętrznej infrastrukturze korporacji.



Rys. 1. Zagrożenia płynące z wewnątrz sieci

– SecureAdmin to system monitorowania aktywności użytkowników działający w sposób przeźroczysty na poziomie warstwy sieciowej. Cechy te oznaczają, że wdrożenie systemu SecureAdmin nie wymaga modyfikowania ani rekonfigurowania istniejących aplikacji lub systemów, a jego obecność nie jest widoczna dla użytkowników. Dzięki temu jest to doskonały system uzupełniający monitorowanie aktywności użytkowników wykonywane w oparciu o logi aplikacyjne i systemowe lub też do monitorowania aktywności administratorów – mówi Roman Lewandowski odpowiedzialny za stworzenie pierwszej wersji systemu, który wraz z Michałem Zalewskim, autorem książki „Cisza w sieci", był pomysłodawcą systemu.

System ma dwie unikatowe cechy. Pierwsza to jego przeźroczystość. Jest to urządzenie drugiej warstwy sieciowej (działa jak *bridge* lub *switch*), a więc jego wdrożenie jest zupełnie niewidoczne dla istniejących w korporacji systemów. Cecha ta jest łatwa do osiągnięcia dla podsłuchiwania pakietów nieszyfrowanych, gdyż wówczas pakiety przesyłane w połączeniach nie są w żaden sposób modyfikowane. Wyjątkowość systemu SecureAdmin polega na zapewnieniu przeźroczystości również w trybie analizowania połączeń przy wykorzystaniu metody *Man In The Middle* (MITM). W tym trybie system, wykorzystując mechanizmy IPTables, przekazuje połączenie na lokalny port i symuluje nawiązanie połączenia przez klienta , natomiast sam nawiązuje połączenie z serwerem w imieniu klienta. Sensor podszywa się pod adresy IP prawdziwego serwera i klienta, tak iż jego obecność jest niewidoczna zarówno dla klienta, jak i dla serwera.

Analizowanie ruchu szyfrowanego jest kluczowe z punktu widzenia bezpieczeństwa wewnętrznego, gdyż pracownicy coraz częściej wykorzystują możliwość tunelowania protokołów nieszyfrowanych z wykorzystaniem szyfrowanych w celu oszukania istniejących w sieci mechanizmów zabezpieczających i monitorujących. Obecnie SecureAdmin obsługuje protokoły sieciowe przedstawione w tabeli.

Analizatory poszczególnych protokołów są ładowane jako osobne, niezależne od siebie moduły. Dzięki temu możliwe jest dodawanie nowych analizatorów bez przerywania pracy pozostałych oraz, w razie potrzeby, stworzenie modułów dla nowych protokołów bez ingerowania w system. Dodatkowo SecureAdmin udostępnia API, dzięki któremu każdy może stworzyć analizator nowego protokołu. Jest to szczególnie

istotne w przypadku korporacji, które wykorzystują własne zamknięte protokoły. Dzięki zastosowanemu mechanizmowi mogą same stworzyć wymagane analizatory.

Celem monitorowania ruchu sieciowego i analizowania protokołów w systemie SecureAdmin jest rejestrowanie aktywności użytkowników. Oznacza to, iż dla większości protokołów nie są rejestrowane wszystkie bajty przesłane w monitorowanym połączeniu (chodź jest to możliwe, jeśli zostanie zapewniona odpowiednia infrastruktura informatyczna, umożliwiająca przechowywanie i przetwarzanie takiej ilości informacji), a jedynie informacje o aktywności użytkowników, czyli o wykonanych przez nich czynnościach oraz ich rezultatach. Oprócz informacji szczególnych dla każdego analizowanego połączenia, przedstawionych w tabeli, rejestrowane są następujące informacje:

- czas rozpoczęcia połączenia,
- czas trwania połączenia,
- źródłowy i docelowy adres MAC,
- źródłowy i docelowy adres IP wraz z portem,
- źródłowy i docelowy adres,
- typ protokołu,
- nazwa użytkownika i hasło (o ile są dostępne).

System SecureAdmin posiada moduł wysokiej dostępności (HA), który dzięki zastosowaniu redundantnej architektury, składającej się z dwóch serwerów działających w trybie *fail-over*, zapewnia ciągłość pracy w przypadku awarii jednego z serwerów. Dzięki tej funkcjonalności w momencie wykrycia awarii jednego z serwerów możliwe będzie automatyczne przełączenie komunikacji na drugi serwer. Należy podkreślić, że wszystkie aktywne sesje użytkownika zostaną przeniesione na drugi serwer, umożliwiając kontynuowanie pracy bez konieczności nawiązywania nowej sesji. Dodatkową funkcjonalnością, niezbędną w przypadku tego typu systemu, jest wbudowany elastycznie konfigurowalny system powiadomień, pozwalający na szybką reakcję na incydenty bezpieczeństwa. SecureAdmin jest w stanie reagować na zdarzenia, wysyłając SMS-y, e-maile, powiadomienia WWW lub tak zwanego trapu *Simple Network Management Protocol* (SNMP), który pozwala na poinformowanie o zaistniałej sytuacji innych urządzeń sieciowych.

Podsumowując – system SecureAdmin nie jest remedium na wszelkie problemy z bezpieczeństwem w sieci korporacyjnej. Jest natomiast znakomitym narzędziem wspomagającym egzekwowanie polityki bezpieczeństwa i wykrywanie jej naruszeń, zarówno celowych, jak i nieumyślnych. Produkt ten pozwala także uniknąć bardzo niebezpiecznej sytuacji, w której administrator może zrobić wszystko wewnątrz sieci, a oprócz tego zamazać swoją działalność. SecureAdmin znacząco ogranicza możliwość wykonania szkodliwego działania bez zostania wykrytym, dzięki czemu jest doskonałym środkiem prewencyjnym, który znacząco podnosi poziom bezpieczeństwa składowanych informacji. Przyczynia się to do możliwości opracowania elastycznych, godnych zaufania i bezpiecznych infrastruktur informatycznych, które będą w stanie przetworzyć rosnącą ilość przepływających informacji.

Maciej Wolański
Comarch

STACJA MONITOROWANIA

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.

tylko do końca roku!

SUPER CENA

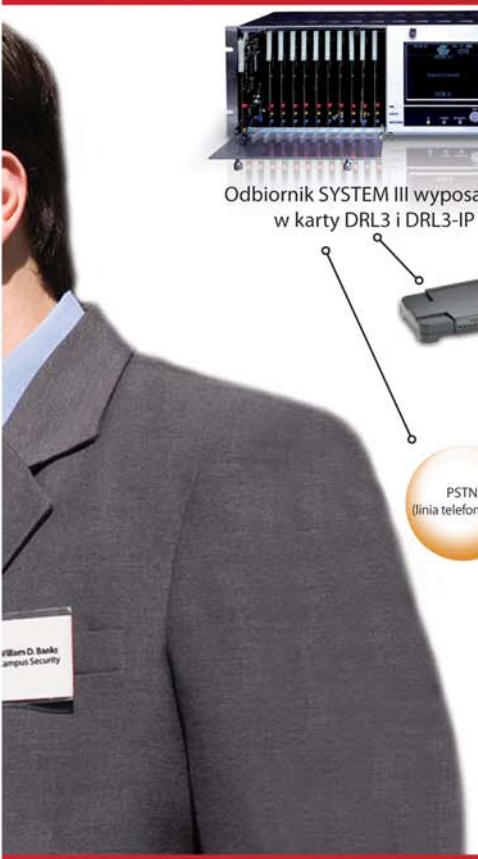
8999* zł

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



KOMPATYBILNE KOMUNIKATORY ALARMOWE

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 1)

Zapraszamy Państwa do cyklu artykułów promujących zarządzanie ryzykiem, który zostanie zamieszczony w kolejnych numerach niniejszego czasopisma dzięki rozpoczętej podczas konferencji *IT Security Management* (Warszawa, 13–14 maja 2008 r.) współpracy z redakcją czasopisma *Zabezpieczenia*. W pierwszym numerze cyklu przekażemy Państwu skrót naszego wykładu z ww. konferencji. Zapraszamy do lektury

Chcielibyśmy przybliżyć Państwu pojęcie zarządzania ryzykiem w prowadzonej działalności gospodarczej, odpowiadając na pytanie: „jaki jest główny cel wprowadzenia właściwego procesu lub procesów zarządzania ryzykiem w firmie?".

Odwołamy się w tym momencie do jakże przekonującej teorii zarządzania ryzykiem skandynawskiej grupy zarządzania ryzykiem Sampo z Helsinek:

„Cele zarządzania ryzykiem to:
- *unikanie katastrof, wypadków, sytuacji mogących narazić firmę na utratę ciągłości jej działania,*
- *optymalizacja kosztów ryzyka"*[1].

Nasz komentarz do pojęcia optymalizacji kosztów ryzyka jest następujący:

„im szybciej zadziałamy, wprowadzając określone procedury, tym mniejsze koszty poniesiemy na redukcję, transfer, zatrzymanie ryzyk czy też na usuwanie strat, a możliwe to będzie tylko przy wprowadzeniu właściwego procesu zarządzania ryzykiem".

Aby dokładnie zrozumieć tę wypowiedź, należy zapoznać się z podstawami teorii ryzyka.

Pragniemy jeszcze zacytować jedno ważne stwierdzenie specjalistów z grupy Sampo, bezpośrednio łączące się z możliwością wystąpienia i z realizacją różnych ryzyk w organizacji:

„W czasach twardej konkurencji jest nawet łatwiej robić pieniądze przez zapobieganie stratom aniżeli przez zwiększanie obrotów (...) W działalności zwyciężają te firmy, które są w stanie zyskać więcej za mniej. Bezpieczeństwo, kontrola strat i zarządzanie ryzykiem są kluczem do uniknięcia strat ludzi, materiałów, czasu, pieniędzy itd."[1].

Co można zawrzeć w stwierdzeniu „itd."? – *„także inne wartości materialne, ale przede wszystkim niematerialne, takie jak know-how, technologia czy inne informacje (aktywa) kluczowe dla firmy".*

Dlaczego temat naszego wystąpienia brzmiał: „Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji"? Bezpieczeństwo informacji ściśle wiąże się bowiem z koniecznością wprowadzenia procedur zarządzania ryzykiem. Przykładem wymagania wprowadzenia takich procedur jest ustanowiona w 2007 r. norma PN-ISO/IEC 27001, w której to rozdział 4 „Ustanowienie i zarządzanie SZBI" traktuje o ryzyku i postępowaniu z nim. Norma ta jest obecnie najpopularniejszym standardem zawierającym wytyczne związane z ustanowieniem i wdrożeniem systemu zarządzania bezpieczeństwem informacji (SZBI), po który chętnie sięgają organizacje, a szczególnie organizacje z branży informatycznej i teleinformatycznej. Jednocześnie pragniemy zwrócić uwagę na fakt, że bezpieczeństwo informacji nie jest tożsame z bezpieczeństwem teleinformatycznym.

Poniżej przytaczamy przykłady informacji prawnie chronionej, do których można zaliczyć:
- dane osobowe,
- tajemnicę służbową,
- tajemnicę bankową,
- tajemnicę ubezpieczeniową,
- tajemnicę państwową (informacja niejawna),
- tajemnicę korespondencji,
- tajemnicę lekarską,
- tajemnicę prawną,
- tajemnicę skarbową.

Często z różnych mediów dowiadujemy się o naruszeniu informacji prawnie chronionej i często po fakcie zadajemy sobie pytanie: „Czy musiało do tego dojść?".

Dodatkowo obligują nas do ochrony tejże informacji takie przepisy prawa, jak np. ustawy o ochronie informacji niejawnych, ochronie danych osobowych, ochronie osób i mienia, ochronie konkurencji i konsumentów, rachunkowości oraz Kodeks Spółek Handlowych.

Aktualnie na świecie funkcjonują różne normy z szeroko pojętego obszaru zarządzania ryzykiem związanym z bezpieczeństwem informacji, z których przytoczona już powyżej najnowsza norma PN-ISO/IEC 27001 jest niczym innym, jak przewodnikiem do wprowadzenia procesów zarządzania ryzykiem w organizacji.

Koncentrując się tylko na obszarze zarządzania ryzykiem systemów teleinformatycznych, za słuszne należy uznać stwierdzenie, że zarządzanie ryzykiem ma na celu zabezpieczenie podstawowych atrybutów informacji w tych systemach, do których należą:
- poufność,
- integralność,
- dostępność,
- autentyczność,
- rozliczalność,
- niezaprzeczalność,
- niezawodność.

1) Kurs podyplomowy zarządzania ryzykiem Wyższej Szkoły Ubezpieczeń i Bankowości, Warszawa, 2000-2001

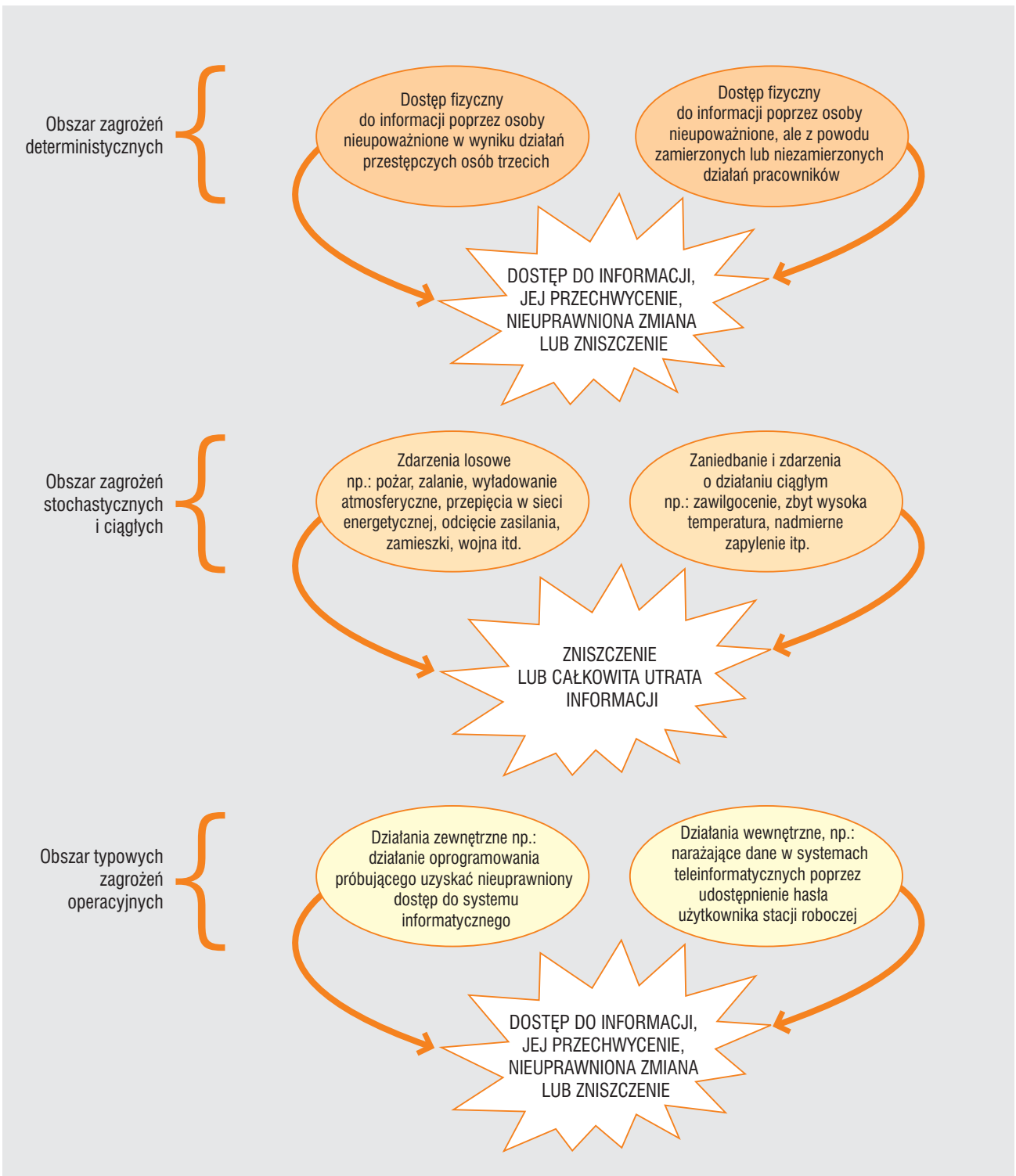
Należy przy tym zabezpieczać informację zarówno za pomocą środków fizycznych, jak i organizacyjnych.

Aby móc zarządzać ryzykiem w organizacji, musimy zapoznać się z kilkoma podstawowymi pojęciami z zakresu teorii ryzyka. I tak:

– **ryzyko** – to kombinacja prawdopodobieństwa wystąpienia zdarzenia oraz jego skutków; ryzyko zawsze wiąże się ze zdarzeniem będącym przyczyną (zagrożenie) i z zespołem warunków, w jakich to zagrożenie się realizuje (podatność);
– **zagrożenie** – to potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub w organizacji;
– **podatność** – to słabość aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie.

Na rysunku 1 przedstawiono trzy przykładowe obszary zagrożeń mogących spowodować ryzyko związane z bezpieczeństwem informacji. Potraktujmy te schematy jako przykłady grup zagrożeń.

Przytoczona definicja ryzyka pochodzi z przewodnika ISO/IEC Guide, 73:2002, w którym znajduje się nomenklatura dotycząca praktycznie wszystkich obszarów, w których chcemy



Rys. 1. Przykładowe obszary zagrożeń dla informacji

wprowadzić procesy zarządzania ryzykiem. Istnieje również wiele innych definicji tego pojęcia, których wybrane przykłady przytaczamy poniżej.

Ryzyko w ujęciu subiektywnym

„Ryzyko jest pewną obiektywną prawidłowością cechującą świat realny, którą jednostka subiektywnie postrzega i interpretuje, i wyrażana jest poprzez niepewność wystąpienia określonych skutków stanu natury”[2].

Ryzyko w ujęciu psychologicznym

„Ryzyko jest stanem umysłu człowieka, jeżeli stan umysłu się zmieni, to zmieni się również ryzyko. Ryzyko istnieje o tyle, o ile podmiot ma świadomość istnienia ryzyka”[2].

Ryzyko z perspektywy szacowania przyszłości

„Ryzyko jest niepewnością przewidywania zdarzeń w przyszłości, wynikającą z niepełności i niedokładności danych statystycznych, na podstawie których dokonuje się szacowania przyszłości”[2].

Ryzyko systemów informatycznych

„Ryzyko systemów informatycznych to zagrożenie, iż technologia informatyczna stosowana w danej organizacji (niezależnie od jej rodzaju i skali działalności) nie spełnia wymogów biznesowych, nie zapewnia odpowiedniej integralności, bezpieczeństwa oraz dostępności danych, nie została odpowiednio wdrożona i nie działa zgodnie z założeniami”[2].

Ryzyko w ujęciu normy PN–I–13335–1:1999

„Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych”

„Ryzyko systemów informatycznych jest zbiorczą miarą prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu, a zatem pośrednią lub bezpośrednią szkodę dla organizacji”[2].

2) Mirosław Ryba, wykład Ernst&Young na temat *”Analiza i zarządzanie ryzykiem systemów informatycznych”*, www.mimuw.edu.pl/~sroka/archiwalne/2005ey/materialy/ey2.pdf

Pokazaliśmy, że ryzyko można kwalifikować w różny sposób, tworząc przy tym różne jego definicje w zależności od specyfiki obszaru, w którym będziemy tym ryzykiem zarządzać.

Mówiąc o zarządzaniu ryzykiem, należy przytoczyć jego definicję. Zgodnie z przewodnikiem ISO/IEC Guide, 73:2002 **zarządzanie ryzykiem** to koordynowane działania kierowania i kontrolowania organizacji z uwzględnieniem ryzyka. A jakie działania? Jednym ze spektakularnych przykładów takich działań jest ciągła analiza ryzyka i reakcja na nie w formie dostosowywania odpowiednich zabezpieczeń.

Widzimy, że zarządzanie ryzykiem jest tak naprawdę zarządzaniem organizacją z uwzględnieniem ryzyka, które może przełożyć się na cel biznesowy. A efekty w postaci apetytu na ryzyko zależą od wielkości i kultury organizacji.

Zapraszamy do zapoznania się z następnymi artykułami, w których zostanie poruszona tematyka modeli zarządzania ryzykiem obecnie funkcjonujących i promowanych przez wiele organizacji zarówno krajowych, jak i europejskich i światowych, tematyka funkcjonujących standardów zarządzania ryzykiem, metodologii szacowania i analizy ryzyka, jak również stosowanych zabezpieczeń obszarów w celu ograniczenia ryzyk obszarów organizacji.

Anna Słodczyk
Piotr Mąkosa
Risk Management Team Poland

Literatura:

1. ISO/IEC Guide, 73:2002 – Risk management – Vocabulary – Guidelines for use in standards.
2. PN-ISO/IEC 17799:2003 – *Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji*.
3. PN-ISO/IEC 27001:2007 – *System zarządzania bezpieczeństwem informacji – wymagania*.
4. PN-I-13335-1:1999 – *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych*.

artykuł sponsorowany

Edge – rozwiązanie kontroli dostępu IP nowej generacji

W dzisiejszych czasach bezpieczeństwo to priorytet każdego przedsiębiorstwa. W większości z nich technicznymi systemami bezpieczeństwa zajmuje się jednak inny dział niż odpowiadający za bezpieczeństwo danych dział IT. W konsekwencji administracja przedsiębiorstwa dysponuje różnymi danymi – często zbędnymi lub nie powiązanymi ze sobą i dotyczącymi zupełnie odrębnych systemów i technologii. Tradycyjne metody połączenia dwóch działów okazały się niepożądane, kosztowne i utrudniały dalszy rozwój. Efektem tego modelu jest słaba kooperacja obu tych działów. W rezultacie rozpowszechnienia się komunikacji IP wzrosły możliwości ujednolicenia systemów bezpieczeństwa w firmach. Dzisiejsza technologia umożliwia systemowe zarządzanie budynkiem z wykorzystaniem skomputeryzowanego systemu, który umożliwia wgląd we wszystkie dostępne funkcje i spina je w jedną całość, poczynając od fizycznej kontroli dostępu przez otwarcie drzwi oraz identyfikację pracowników, a kończąc na logicznym systemie bezpieczeństwa. Rozwiązania kontroli dostępu nowej generacji umożliwiają urealnienie takiego futurystycznego scenariusza. Firma HID Global podjęła to wyzwanie i przedstawia rodzinę produktów Edge opartych na rozwiązaniach dostępowych IP

Zalety systemowego zarządzania bezpieczeństwem przez dział IT

HID Global dostarcza rozwiązań, które służą do integracji systemów fizycznej (PACS – ang. ***Physical Access Control***) i logicznej kontroli dostępu (LACS – ang. ***Logical Access Control***). Rozwiązania te zapewniają wielowarstwową ochronę przedsiębiorstwa. Co ważniejsze, łączą aktywa, wydatki oraz umiejętności personelu dwóch wymienionych wyżej działów.

Poniżej przedstawiono kilka powodów, dla których powierzenie działowi IT integracji systemów bezpieczeństwa jest atrakcyjne.

Zarządzanie IT a budżet

Zadania stawiane przed działem IT to wykorzystanie technologii do pozyskiwania, ochrony i transmisji informacji w przedsiębiorstwach oraz zarządzania nią. Z uwagi na to, że wiele działów funkcjonalnych w przedsiębiorstwach, związanych np. z komunikacją, przetwarzaniem danych czy finansami, widzi w technologii drogę do upraszczania procedur, zaufanie, jakim obdarzają one dział IT, daje mu znaczny wpływ na decyzje budżetowania. Dział IT sam dokonuje wyborów sprzętu komputerowego, jego zakupy mogą być bardziej efektywne pod względem kosztów.

Standard

Sukces branży IT polega na standaryzacji – ujednoliceniu technologii, procesów, architektury, okablowania, praktyki w instalacjach, sprzętu komputerowego, zasilania przez Ethernet (PoE) itp. Podczas otwierania nowego biura dział IT jest jednym z pierwszych doradców przy projektowaniu. Produkcja masowa i ujednolicenia znacznie ograniczyły koszty urządzeń, gwarantując jednocześnie większą ich dostępność. Ze względu na konieczność adaptacji do różnych okoliczności komponenty IT promowane są jako dobre rozwiązania do każdego przedsięwzięcia. Konstrukcja standardowych mechanizmów IT pozwala również na ich mobilność przy zmianie platform oprogramowania. Bez wcześniej określonych standardów nie byłoby to możliwe.

To już istnieje

Nacisk na oszczędności w budowaniu infrastruktury IT okazał się kluczem do sukcesu. Firmy zainwestowały już w taką infrastrukturę, mogą więc zaoszczędzić na inwestycjach w przełączniki i zasilanie (UPS).

Zwiększenie szybkości instalacji

Systemy bezpieczeństwa zawsze były zamknięte pod względem infrastruktury kablowej. W rozwiązaniach tradycyjnych do podłączenia kontrolera przy drzwiach wymaganych było 16 różnych kabli. Okablowanie IT – typowo kategorii 5 – wykorzystuje jedynie cztery pary „inteligentnych" przewodów: dwie pary kabli zasilających i dwie pary do zapewnienia komunikacji. Ten rodzaj okablowania jest łatwiejszy w instalacji i bardziej wydajny niż tradycyjne rozwiązania. Czy nie byłoby warto uczynić standardy okablowania sieciowego dźwignią systemów bezpieczeństwa?

Technologia – możliwości rozwiązań zasilania

Systemy bezpieczeństwa mogą wiele skorzystać z osiągnięć IT w zakresie dystrybucji zasilania. Technologia PoE zapewnia dodatkowe źródło zasilania odległych urządzeń za pomocą skręconej pary kabli sieci Ethernet. Do niedawna okablowanie Ethernet umożliwiało jedynie przesyłanie danych. Do zasilania urządzeń systemów bezpieczeństwa wymagane było dodatkowe źródło zasilania wraz z dodatkowym okablowaniem. Wykorzystanie PoE redukuje koszty i czas instalacji oraz gwarantuje jej kompleksowość.

Wykonanie

Struktura IT chroni lepiej dane przedsiębiorstwa umieszczane w sieci. Ze względu na zawartość danych krytycznych

infrastruktura sieci IT jest w pełni monitorowana, ma również zapewnione zasilanie zapasowe (UPS).

Możliwości produktów rodziny Edge

Powyższe zalety systemów bazujących na rozwiązaniach IT zostały wykorzystane przez firmę HID w urządzeniach Edge – rodzinie rozwiązań przeznaczonych do systemów kontroli dostępu. Platforma Edge firmy HID Global to procesor kontroli dostępu z komunikacją IP oraz interfejs komputerowy. Jego konstrukcja zapewnia kompletny zestaw cech typowych dla systemów kontroli dostępu pod względem wykorzystanych komponentów, oprogramowania oraz zdolności odczytu/zapisu inteligentnych kart zbliżeniowych.

Produkty Edge zawierają również wieloplatformową technologię OPIN, nową otwartą architekturę, pozwalającą im na pełną integrację z dowolnym systemem kontroli dostępu, wykorzystującym interfejs komunikacyjny IP. Elastyczne rozwiązanie sprowadza inteligencję systemu do poziomu zabezpieczanego przejścia i pozwala na integrację z czytnikami iCLASS oraz umożliwia komunikację z czytnikami w formatach Wiegand lub Clock & Data.

Produkty Edge są doskonałe do instalacji w nowych obiektach. Wymagają mniej okablowania, są efektywne pod względem kosztów – wręcz idealne do dzisiejszego środowiska systemów bezpieczeństwa bazujących na rozwiązaniach IT. W przypadku starszych systemów zawarta w produktach Edge technologia OPIN umożliwia wykorzystanie przez nie przyszłych rozwiązań oprogramowania komputerowego bez konieczności instalacji dodatkowych urządzeń, przez co systemy takie można dostosować do zmieniających się potrzeb przedsiębiorstwa w zakresie systemów bezpieczeństwa.

Edge Solo to urządzenia przeznaczone do złożonych lub pojedynczych instalacji kontroli przejść. Z wbudowanym interfejsem użytkownika system Edge Solo może działać bez aplikacji komputerowych. Dzięki technologii OPIN oprogramowanie urządzenia Edge Solo może zostać poszerzone w celu zintegrowania z systemem bardziej rozbudowanym, który wykorzystuje taką aplikację.

Edge Host to rozwiązanie zaprojektowane do większych systemów – z setkami kontrolowanych drzwi i urządzeń powiązanych z firmowym systemem oprogramowania. Dla obu tych wersji (Solo i Host) firma HID proponuje wielofunkcyjne czytniki ERW400, ER40 i ESR40 oraz kontrolery drzwiowe E400 i ES400, pozwalające użytkownikowi dobrać czytniki zgodnie z potrzebami.

Czesław Półtorak
HID Global

artykuł sponsorowany

SynopSYS

Integracja systemów bezpieczeństwa i komfortu

Dotychczasowa praktyka wskazuje, że w większości budynków systemy bezpieczeństwa i komfortu są realizowane oddzielnie. Co więcej, poszczególne elementy tych systemów są także oparte na odrębnych instalacjach. Taki stan rzeczy ma określone konsekwencje. Już na etapie realizacji samo okablowanie jest zdecydowanie droższe i bardziej skomplikowane. Eksploatacja takich rozwiązań to konieczność współpracy z wieloma dostawcami oraz wydłużenie czasu szkoleń operatorów, w celu wdrożenia ich do pracy z różnymi interfejsami użytkownika. Dodatkowym problemem jest wymiana informacji między systemami, co szczególnie w warunkach kryzysowych może stać się przyczyną podniesienia poziomu zagrożenia, a w konsekwencji doprowadzić do zwiększenia strat. W poniższym materiale pragniemy przedstawić rozwiązania, jakie w tym zakresie oferuje swoim partnerom firma RISCO Group.

Nowe technologie a integracja

Jeszcze do niedawna systemy zabezpieczeń elektronicznych i systemy automatyki budynków były traktowane jako oddzielne, bez fizycznej ani logicznej możliwości łączenia ich funkcji. Sytuacja ta zmieniła się. W dzisiejszych czasach osoby administrujące systemami zarządzania budynkami mają do dyspozycji narzędzia programowe pozwalające traktować obiekt (zarówno skupiony – pojedynczy budynek, jak i rozproszony – kompleks budynków lub obiektów) jako jedną całość. Takie podejście zapewnia oczywiście wygodę użytkowania, a ponadto pozwala na znaczące oszczędności zarówno w przypadku kosztów personalnych, jak i wydatków na energię.

Koncepcja ta stała się możliwa dzięki rozwojowi i powszechnej akceptacji kilku technologii bazujących na dostępnych standardach, na których oparto platformy programowe. Należy do nich zaliczyć protokół TCP/IP, czyli faktyczny standard komunikacji w sieciach komputerowych, oraz technologię UPnP ***(Universal Plug & Play)***. Korzyści wynikające ze stosowania otwartych standardów to przede wszystkim łatwiejsza integracja między programami, uproszczona wymiana informacji oraz niezależność od dostawców. Technologia UPnP zlikwidowała ostatnie bariery na drodze spójności systemów zabezpieczeń i automatyki, dając do dyspozycji uniwersalny język komunikacji pomiędzy wszelkiego rodzaju systemami. Umożliwia on prostą komunikację między urządzeniami różnych dostawców i pozwala na ich integrację oraz kontrolę, pozwalając powszechnie stosowanym urządzeniom, takim jak elementy oświetlenia, klimatyzatory, grzejniki i windy, jak również systemom bezpieczeństwa, porozumiewać się ze sobą.

SynopSYS – interfejs użytkownika

Wykorzystując wspomniane technologie, można zintegrować systemy bezpieczeństwa i zarządzania budynkiem w jeden organizm, w którym różne komponenty bez problemów współdziałają ze sobą, a całość jest nadzorowana z poziomu jednego, wspólnego interfejsu użytkownika. Takim rozwiązaniem jest oprogramowanie **SynopSYS** firmy RISCO Group. Dzięki najnowocześniejszym rozwiązaniom informatycznym SynopSYS łączy systemy sygnalizacji włamania, napadu, pożaru, kontrolę dostępu, monitoring wizyjny, sterowanie ogrzewaniem, wentylacją, klimatyzacją i innymi systemami automatyki w jedno stanowisko nadzoru i sterowania obiektem.

Najważniejsze właściwości tego oprogramowania to:

- praca w sieciach LAN/WAN z centralnym serwerem baz danych,
- bezpieczeństwo – najwyższy komercyjny poziom bezpieczeństwa przesyłu danych przez IP, wykorzystujący najnowocześniejsze algorytmy kryptograficzne,
- zgodność ze standardem UPnP – natychmiastowa komunikacja z urządzeniami,
- otwarta architektura – prosta integracja z dowolnymi systemami,
- budowa modułowa – dobór urządzeń niezbędnych dla konkretnej instalacji,
- proste tworzenie planów sytuacyjnych – gotowe biblioteki symboli graficznych urządzeń w połączeniu z ułatwieniami programowymi.

SynopSYS zapewnia dostęp do informacji w czasie rzeczywistym – w dowolnym miejscu i czasie – umożliwiając tym samym inteligentną integrację i analizę informacji oraz pozwalając na zautomatyzowanie procesów w całym budynku, jak również w grupach budynków o różnym przeznaczeniu. Z poziomu tego pojedynczego interfejsu operatorzy mogą zarządzać szerokim wachlarzem zdefiniowanych funkcji obejmujących kontrolę środowiska, kontrolę dostępu, nadzór wideo, SSWiN itp. Dodatkowe korzyści to uproszczona kontrola odległych miejsc, przyspieszenie reakcji na sytuacje alarmowe oraz podniesienie poziomu skuteczności całego systemu.

Z punktu widzenia inwestora dzięki oprogramowaniu SynopSYS cały chroniony obszar – czy będzie to pojedynczy budynek, czy zespół rozproszonych obiektów – może być monitorowany i sterowany z pojedynczego stanowiska obsługi, wyposażonego w standardowy komputer, co pozwala na redukcję kosztów osobowych przy jednoczesnym zwiększeniu wydajności obsługi. Ponadto system w sposób znaczący przyczynia się do redukcji kosztów eksploatacji budynku – dzięki automatycznemu sterowaniu oświetleniem, ogrzewaniem i klimatyzacją w okresowo nieużywanych pomieszczeniach.

Jak wspomniano powyżej, oprogramowanie SynopSYS może być zastosowane zarówno w pojedynczych obiektach, jak też w grupach obiektów. Duża elastyczność tego rozwiązania pozwala na realizację zintegrowanych systemów w obiektach o bardzo różnym charakterze – doskonale nadaje się zarówno do obiektów komercyjnych, użyteczności publicznej, dużych kompleksów, jak i do obiektów rozproszonych.

RISCO Group Poland
ul. 17 Stycznia 56
02–146 Warszawa
tel: (22) 500 28 40, faks: (22) 500 28 41
www.riscogroup.com, e-mail: sales-pl@riscogroup.com

RACS ROGER ACCESS CONTROL SYSTEM

seria radius

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 125kHz lub 13.56MHz Mifare. Nową kategorię produktów stanowi wandalo-odporny czytnik zbliżeniowy (PRT64VP) w którym zarówno przednia część obudowy jak i klawisze są wykonane w całości z metalu.
Na szczególną uwagę zasługuje również kontroler PR602LCD, który został specjalnie zaprojektowany dla systemów rejestracji czasu pracy (RCP) co nie wyklucza jednak możliwości stosowania go jako zwykłego kontrolera dostępu. Urządzenia rodziny Radius mogą być instalowane na zewnątrz budynków i są kompatybilne z wcześniej produkowanymi kontrolerami dostępu serii PR oraz czytnikami PRT, mogą one być dołączane do istniejących już systemów kontroli dostępu pracujących autonomicznie lub pod kontrolą programu PR Master (*).

(*) **Informacja**
Począwszy od 1 września 2007 program PR Master jest rozprowadzany z darmową licencją bez ograniczenia liczby kontrolerów w systemie.

CE

profesjonalna kontrola dostępu

roger®
www.roger.pl

WYMAGANIA W ZAKRESIE BEZPIECZEŃSTWA OKIEN I DRZWI WYNIKAJĄCE Z NORM EUROPEJSKICH

Obiekt budowlany może zagrażać bezpieczeństwu, zdrowiu i mieniu użytkownika, jeżeli został niewłaściwie zaprojektowany lub wykonany oraz gdy do jego wznoszenia zastosowano niewłaściwe wyroby budowlane. Zagadnienia bezpieczeństwa użytkowania oraz zdrowia objęte są rozporządzeniem Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. Nr 75, poz. 690 z późniejszymi zmianami)

Wprowadzenie

Rozporządzenie to nie reguluje jednak zagadnień ochrony użytkowników budynków przed utratą mienia w wyniku włamania. Ta cecha użytkowa obiektów regulowana jest jedynie przepisami ustalonymi przez poszczególne firmy ubezpieczeniowe, które określają m.in. ogólne wymagania w zakresie odporności na włamanie.

Jednymi z elementów budynku najbardziej narażonych na dokonywanie przez nie włamania są okna i drzwi. W związku z tym coraz częściej stosuje się okna i drzwi utrudniające włamanie, które przeznaczone są do tego, aby w stanie wbudowanym i zamkniętym w wystarczającym stopniu utrudnić okazjonalnemu włamywaczowi dokonanie włamania, przy czym bierze się pod uwagę zwykle stosowane przez niego narzędzia.

Okna i drzwi są wyrobami budowlanymi, których wprowadzenie do obrotu powinno być zgodne z wymaganiami Ustawy z dnia 16 kwietnia 2004 r. o wyrobach budowlanych (Dz. U. Nr 92, poz. 881), wdrażającej postanowienia Dyrektywy 89/106/EWG z dnia 21 grudnia 1988 r. w sprawie zbliżenia ustaw i aktów wykonywanych Państw Członkowskich dotyczących wyrobów budowlanych. W powyższej ustawie zawarto stwierdzenie, że wyrób nadaje się do stosowania przy wykonywaniu robót budowlanych, jeżeli dokonano oceny jego zgodności z normą zharmonizowaną lub aprobatą techniczną. Takim dokumentem w odniesieniu do drzwi i okien jest wdrożona w 2006 r. do Katalogu Polskich Norm zharmonizowana norma europejska PN-EN 14351-1:2006 „Okna i drzwi. Norma wyrobu, właściwości eksploatacyjne. Część 1: Okna i drzwi zewnętrzne bez właściwości dotyczących odporności ogniowej i/lub dymoszczelności”.

Przedstawiona norma obejmuje także problematykę związaną z wymaganiami i badaniami, odnoszącą się do odporności okien i drzwi na włamanie.

Zakres ogólny norm dotyczący odporności na włamanie okien i drzwi

Norma PN-EN 14351-1:2006 na okna i drzwi zewnętrzne zawiera w p. 4.23 stwierdzenie, że zagadnienia odporności na włamanie tych wyrobów powinny być zgodne z serią norm ENV.

W 1997 roku Europejski Komitet Normalizacyjny (CEN) przyjął pakiet norm przeznaczonych do tymczasowego stosowania dotyczących odporności na włamanie okien, drzwi i żaluzji. Normy przeznaczone do tymczasowego stosowania oznaczane są jako ENV i zwane są także prenormami europejskimi. W uzasadnieniu nadania tym dokumentom statusu normy do tymczasowego stosowania podano, że wynika to z faktu nieposiadania przez większość państw należących do CEN doświadczenia w badaniach z zastosowaniem prób włamania ręcznego. Faza stosowania ENV daje wszystkim możliwość zdobycia doświadczenia w stosowaniu prenormy, wymiany uzyskanych doświadczeń i harmonizacji procedur. Możliwe jest także określenie, czy część badań metodami prób ręcznych będzie mogła być zastąpiona przez metody o wyższym stopniu odtwarzalności.

W skład pakietu norm przeznaczonych do tymczasowego stosowania w zakresie odporności na włamanie okien, drzwi i żaluzji weszły:

- ENV 1627 – Okna, drzwi, żaluzje – Odporność na włamanie – Wymagania i klasyfikacja,
- ENV 1628 – Okna, drzwi, żaluzje – Odporność na włamanie – Metoda badania dla określenia odporności na obciążenie statyczne,
- ENV 1629 – Okna, drzwi, żaluzje – Odporność na włamanie – Metoda badania dla określenia odporności na obciążenie dynamiczne,
- ENV 1630 – Okna, drzwi, żaluzje – Odporność na włamanie – Metoda badania dla określenia odporności na próby włamania ręcznego.

Poszczególne normy obejmują następujący zakres:

ENV 1627 określa wymagania i klasyfikację dla właściwości dotyczących odporności na włamanie drzwi, okien oraz żaluzji i ma zastosowanie do wyrobów posiadających następujące sposoby otwierania: rozwieranie, przechylanie, składanie, rozwieranie – uchylanie, górne lub dolne zawieszenie, przesuwanie poziome lub pionowe oraz zwijanie,

ENV 1628 precyzuje metodę badania dla określenia odporności na obciążenie statyczne w celu oceny właściwości przeciwwłamaniowych okien, drzwi i żaluzji,

ENV 1629 podaje metodę badania dla określenia odporności na obciążenie dynamiczne w celu oceny właściwości przeciwwłamaniowych okien, drzwi i żaluzji,

ENV 1630 podaje metodę badania dla określenia odporności na próby włamania ręcznego w celu oceny właściwości przeciwwłamaniowych okien, drzwi i żaluzji, niezależnie od materiału, z jakiego zrobiono te wyroby, oraz przedstawia zestawy narzędzi.

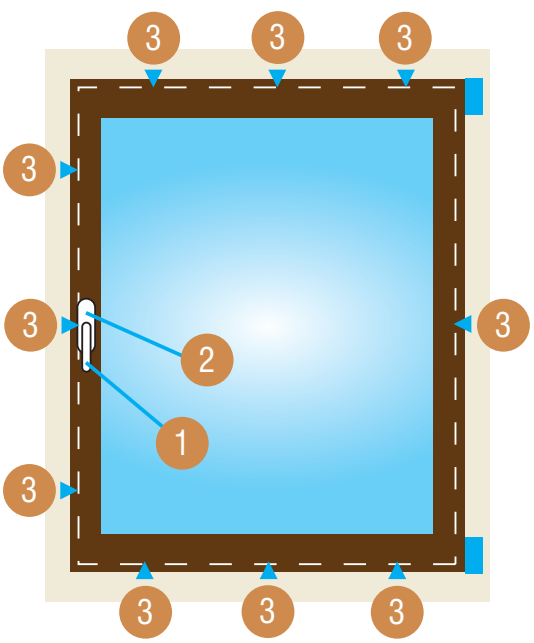
Wyszczególnione normy zostały opublikowane w styczniu 1999 roku z zapisem, że okres ich ważności wstępnie ogranicza się do trzech lat. Okres ten minął w 2002 roku i wtedy też właściwy Komitet Techniczny CEN TC 33 („Okna, drzwi, bramy, żaluzje, okucia budowlane i ściany osłonowe") na bazie doświadczeń uzyskanych w eksperymentalnym stosowaniu podjął decyzję o przedłużeniu ich ważności na kolejne dwa lata, a następnie rewizji tych prenorm z zamiarem przekształcenia w normy EN. Obecnie trwają w dalszym ciągu prace normalizacyjne związane z projektami tych norm.

W Polsce w roku 2006 wprowadzono do katalogu Polskich Norm powyższe prenormy oznaczone jako PN-ENV 1627:2006, PN-ENV 1628:2006, PN-ENV 1629:2006 i PN-ENV 1630:2006, które są dostępne tylko w języku oryginału.

W prezentowanych prenormach zawarte są definicje związane z ich zakresem.

Najważniejsze z nich to:

a) odporność na włamanie: właściwość okna, drzwi lub żaluzji polegająca na stawianiu oporu próbom wtargnięcia do chronionego pomieszczenia lub obszaru (wskutek zastosowania fizycznej przemocy, za pomocą określonych z góry narzędzi, okno, drzwi lub żaluzja zostają uszkodzone lub zniszczone);



Rys. 1. Przykład okna rozwieranego w stanie zamknięcia, utwierdzenia i zablokowania (1 - klameczka, 2 - mechanizm blokujący klameczkę z kluczem, 3 - punkt utwierdzenia wielopunktowego mechanizmu zamykającego)

b) elementy przeciwwłamaniowe (odporne na włamanie): kompletne, funkcjonujące elementy, które spełniają wymagania poszczególnych prenorm europejskich; elementy te – gdy są wbudowane i utwierdzone lub utwierdzone i zablokowane – pełnią funkcję oporu przeciw wtargnięciu dokonanemu przy użyciu fizycznej przemocy wspomaganej przez określone z góry narzędzia;

c) klasa odporności: poziom odporności na próby włamania, którą zapewnia okno, drzwi lub żaluzja;

d) próbka do badań: kompletne, funkcjonujące okno, drzwi lub żaluzja;

e) strona ataku: strona próbki do badań, określona przez zgłaszającego jako strona narażona na atak;

f) stan zamknięcia i utwierdzenia: stan, w którym okno, drzwi lub żaluzja są zabezpieczone w taki sposób, że mogą być otwarte od wewnątrz bez klucza

i bez jakiegokolwiek uszkodzenia, ale nie mogą być one otwarte od strony ataku;

g) stan zamknięcia, utwierdzenia i zablokowania: stan, w którym okno, drzwi lub żaluzja są zabezpieczone w taki sposób, że nie mogą być otwarte z obydwu stron bez klucza lub urządzenia elektrycznego i bez jakiegokolwiek uszkodzenia – przykład na rysunku 1;

h) czas oporu: czas roboczy osoby badającej i przeprowadzającej próbę włamania ręcznego, liczony łącznie z czasami zmiany narzędzi krótszymi niż 5 s każdy, np. przy zmianie wkrętaka na łom stalowy;

i) całkowity czas badania: kombinacja czasów oporu, czasów wypoczynku, czasów wymiany narzędzi i czasów obserwacji.

Próby badania włamania ręcznego polegają na utworzeniu w wyrobie otworu dostępu, który pozwala na przejście bloku testowego o przekroju poprzecznym mającym którykolwiek z następujących wymiarów:

– prostokąt o wymiarach 400 x 250 mm lub
– elipsę o wymiarach 400 x 300 mm lub
– koło o średnicy 350 mm.

Wymagania i klasyfikacja w zakresie odporności na włamanie okien i drzwi

Producent występujący o ustalenie klasy odporności na włamanie okna lub drzwi powinien w pierwszej kolejności określić, który ze stanów zamknięcia (definicja podana w pozycjach f i g poprzedniego rozdziału) przewiduje dla swojego wyrobu.

Zgłaszając się do badań, producent powinien dostarczyć do laboratorium badawczego następującą dokumentację:

– szczegółowe rysunki,
– wykaz części,
– wykaz wszystkich dostępnych wymiarów okna lub drzwi,
– wszystkie dostępne dokumenty określające parametry okuć, uszczelek i innych akcesoriów (aprobaty techniczne, certyfikaty, raporty z badań itp.),
– instrukcję instalowania (zabudowy) okna lub drzwi opracowaną przez producenta

oraz

– określić strony ataku,
– zadeklarować klasę odporności, którą przewiduje dla swojego wyrobu.

W załączniku do normy PN-ENV 1627:2006 podano przykładową zawartość instrukcji instalowania. Instrukcja powinna zawierać co najmniej:

a) typowe szczegóły dotyczące otworów budowlanych, w które wyrób ma być wbudowany;

b) szczegóły dotyczące podstawowych punktów zamocowania, jak również dokładny opis elementów mocujących;

c) wskazanie punktów, które wymagają szczególnie sztywnego zamocowania, jak np. najbliższe otoczenie zamków i zawiasów;

d) wskazania dotyczące niezbędnego zasięgu zagęszczonego wypełnienia oporowego wnęki pomiędzy ścianą a ościeżnicą, np. w okolicach zamków i zawiasów;

e) wskazania dotyczące szczelin, które mają zostać zachowane pomiędzy częściami ruchomymi a nieruchomymi;

f) wskazania dotyczące maksymalnego dopuszczalnego wystawania wkładki bębenkowej poza zewnętrzną tarczę osłaniającą zamek – tam, gdzie ma to zastosowanie;

g) inne szczegóły, wraz z określeniem na ile wpływają one na właściwości przeciwwłamaniowe próbki do badań;

Okna i drzwi o określonej odporności na włamanie powinny, zgodnie z normą PN-ENV 1627:2006, spełniać poniżej wymienione wymagania.

Oszklenie i inne wypełnienia

Zamocowania oszklenia lub innych wypełnień powinny być tak skonstruowane, aby były w stanie wytrzymać obciążenia statyczne i dynamiczne oraz próby włamania ręcznego, jak również powinny uniemożliwiać ich usunięcie od strony ataku.

Cel ochrony	Rodzaj okucia	Klasa odporności wg PN-ENV 1627:2006	Wymagania	Parametry badania
Ochrona przed wierceniem	Skrzynka zamka (okno)	1 – 6	Skrzynka zamka zabezpieczona przed wierceniem lub warstwa zabezpieczona przed wierceniem lub okucie osłonowe zabezpieczone przed wierceniem zachodzące na skrzynkę	Czas wiercenia netto – 50% czas oporu zgodnie z tab. 4, ale co najmniej 3 min
Ochrona przed przemieszczeniem czopa zamykającego okuć okiennych	Okucia rozwierane, uchylne i uchylno-rozwierane	1 – 6	Czop zamykający jest obciążony w kierunku przeciwnym do zamknięcia siłą F2 maksimum 6 kN	Czop zamykający może być cofnięty najwyżej o 50% drogi zamykania
Ochrona przed oderwaniem	Klamka okienna z blokadą	1 – 6	Klamka okienna jest obciążona prostopadle w stosunku do płaszczyzny jej obrotu momentem obrotowym 100 Nm	Nie powinny wystąpić żadne uszkodzenia uniemożliwiające otwarcie okna poprzez system transmisyjny
Ochrona przed ukręceniem	Klamka okienna z blokadą	1 – 6	Zablokowana klamka okienna jest obciążona momentem obrotowym 100 Nm, przeciwnym do kierunku zamykania	Klamka okienna nie powinna zostać obrócona do pozycji otwarcia, ani wyłamać się w ten sposób, aby zostało osiągnięte otwarcie okna

Tab. 1. Wymagania dotyczące okien o określonej klasie odporności na włamanie

ALBERT
THE VIDEO AGENT

ULISSE
WBUDOWANE SYSTEMY LOKALIZUJĄCE

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.

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

Zainstalowane w oknach i drzwiach szyby powinny spełniać, w zależności od klasy odporności wyrobu, wymagania przewidziane dla klasy odporności oszklenia od P4A do P8B według normy PN-EN 356:2000 „Szkło w budownictwie. Szyby ochronne. Badania i klasyfikacja odporności na ręczny atak".

Wymagania dla okuć

Wszystkie okucia, w które wyposażone jest okno lub drzwi, powinny być zdolne do zapewnienia stanu zamknięcia i utwierdzenia. Okucia przeszklonych wyrobów w 1 klasie odporności, nie mających oszklenia bezpiecznego, zgodnego z normą PN-EN 356:2000, powinny być zdolne do zapewnienia stanu zablokowania.

Okucia powinny spełniać zadania zabezpieczające, podane w załączniku C normy PN-ENV 1627:2006. W tabeli 1, stanowiącej wyciąg z załącznika C, przedstawiono wymagania dotyczące okien o określonej klasie odporności na włamanie.

Wymagania dotyczące wytrzymałości mechanicznej

Obciążenie statyczne

Okno lub drzwi poddane obciążeniu statycznemu (wg metodyki przedstawionej w normie PN-ENV 1628:2006) nie powinny ugiąć się (odchylić) poza granice przedstawione w tab. 2 (dla uproszczenia nie ujęto w niej zagadnień stempla, co występuje w normie PN-ENV 1627:2006, tabela 2).

Klasy odporności	1 i 2		3		4		5 i 6	
Parametry / Punkty i miejsce obciążeń	Obciążenie w kN	Odchylenie w mm	Obciążenie w kN	Odchylenie w mm	Obciążenie w kN	Odchylenie w mm	Obciążenie w kN	Odchylenie w mm
F 1 Naroże, wypełnienia	3	8	6	8	10	8	15	8
F 2 Pomiędzy punktami unieruchomienia	1,5	30	3	20	6	10	10	10
F 3 W punktach unieruchomienia	3[1] lub 6[2]	10	6	10	10	10	15	10

[1] gdy okno lub drzwi wyposażono w system zamknięcia wielopunktowego
[2] gdy okno lub drzwi wyposażono w zamkniecie jednopunktowe

Tab. 2. Wymagania dotyczące obciążeń statycznych okien lub drzwi

Obciążenie dynamiczne

Okno lub drzwi poddane obciążeniu dynamicznemu zgodnemu z tab. 3 nie powinny otworzyć się na tyle, aby umożliwić dostęp do jakichkolwiek mechanizmów blokujących lub pozwolić na powstanie otworu dostępu, a ponadto żadna część jakiegokolwiek wypełnienia lub zamocowań okna lub drzwi nie powinna zostać odłączona lub usunięta.

Jeżeli do wypełnienia okna lub przeszklenia drzwi użyto szkła spełniającego wymagania normy PN-EN 356:2000, wówczas obciążenie w punkcie środkowym należy pominąć. Punktami badania powinny być wszystkie naroża. Szkło może pęknąć podczas próby, ale nie powinien powstać otwór dostępu.

Klasa odporności	Masa elementu uderzającego w kg	Wysokość spadania w mm
1	30	800
2	30	800
3	30	1200

Tab. 3. Wymagania dotyczące obciążeń dynamicznych okien lub drzwi

Badania wykazują, że obciążenia statyczne osiągane w klasach od 4 do 6 są wyraźnie wyższe od osiąganych w badaniach na obciążenia dynamiczne. Ponadto obciążenia dynamiczne wywierają na badany wyrób działanie trwające tylko od 20 do 40 ms, podczas gdy obciążenie statyczne daje działanie trwające 60 s. Z tego powodu autorzy prenormy ENV 1627 pomijają badania dynamiczne dla klas od 4 do 6.

Odporność na próby włamania ręcznego

Podczas próby włamania ręcznego wg procedury przedstawionej w normie PN-ENV 1630:2006, w czasie podanym w tabeli 4, w oknie lub drzwiach nie powinien zostać utworzony otwór dostępu.

Podczas prób włamania ręcznego okien lub drzwi przeszklonych należy także badać zamocowanie szkła.

Klasy odporności

Jeżeli zostaną spełnione wszystkie powyżej przedstawione wymagania dla danej klasy odporności (zgodnie z normą PN-ENV 1627:2006), wówczas oknu lub drzwiom należy przyznać tę klasę odporności na włamanie. Klasy odporności na włamanie wraz z metodami oraz parametrami wymagań przedstawiono w tabeli 4.

Badania

Kolejność i próbki do badań

Kolejność przeprowadzania badań powinna być następująca:
- odporność na obciążenie statyczne zgodnie z normą PN-ENV 1628:2006,
- odporność na obciążenie dynamiczne zgodnie z normą PN-ENV 1629:2006,
- odporność na próby włamania ręcznego – badanie wstępne zgodnie z normą PN-ENV 1630:2006,
- odporność na próby włamania ręcznego – badanie główne zgodnie z normą PN-ENV 1630:2006.

Do klasy odporności 1 wymagane jest dostarczenie jednej próbki do badań.

Próbka użyta w badaniach na obciążenie statyczne i dynamiczne może być również użyta w badaniach wstępnych włamania ręcznego, lecz pod warunkiem, że żadne z uszkodzeń spowodowanych tamtymi badaniami nie wpłynie na wyniki badania wstępnego. Do badania głównego należy bezwzględnie użyć nowej próbki. Wymiary próbki określa laboratorium badawcze, przy czym powinny to być wymiary reprezentatywne dla asortymentu wyrobów.

Próbka do badań powinna być przechowywana w odpowiednim pomieszczeniu tak długo, aż temperatura i zawartość wilgoci (wyroby drewniane) wykażą stabilne wartości, mieszczące się w granicach: temperatura – od 15°C do 30°C, zawartość wilgoci – od 5% do 18%.

Klasa odporności	Przewidywana metoda włamania rabunkowego	Parametry wymagań przy próbie włamania ręcznego		
		Zestaw narzędzi	Czas oporu w min	Całkowity czas badania w min
1	Przypadkowe próby włamania poprzez rozbicie okna lub drzwi przy użyciu przemocy fizycznej, np. kopania, napierania barkiem, podnoszenia, wyrywania itp.	Bez badań na włamanie ręczne		
2	Przypadkowe próby włamania poprzez rozbicie okna lub drzwi z dodatkowym użyciem prostych narzędzi, np. śrubokręta, szczypców, klina	A	3	15
3	Próby włamania rabunkowego przy użyciu dodatkowego śrubokręta oraz łomu stalowego	B	5	20
4	Włamanie oparte na doświadczeniu, przy dodatkowym użyciu pił, młotków, siekier, dłut oraz przenośnych bateryjnych wiertarek z napędem silnika	C	10	30
5	Włamanie poparte doświadczeniem, z dodatkowym użyciem narzędzi elektrycznych, np. wiertarek, wyrzynarek (do drewna), przenośnych pił oraz szlifierek kątowych z maks. średnicą tarczy 125 mm	D	15	40
6	Włamanie oparte na doświadczeniu, z dodatkowym użyciem narzędzi elektrycznych dużej mocy, np. wiertarek, wyrzynarek, pił oraz szlifierek kątowych z tarczami o maks. średnicy 230 mm	E	20	50

Tab. 4. Klasy odporności na włamanie

Badanie odporności na obciążenie statyczne

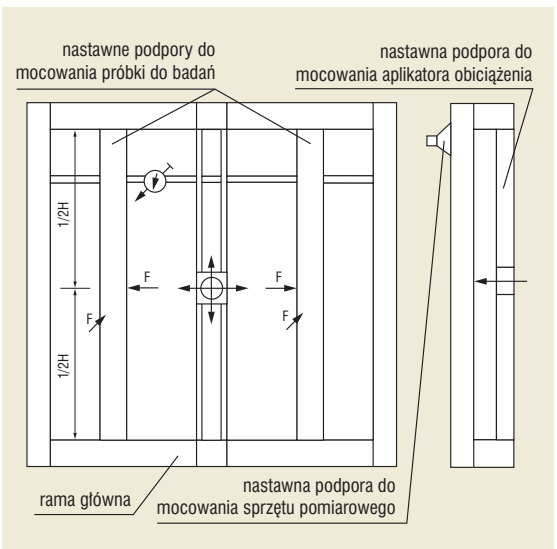
Badanie przeprowadza się na urządzeniu, które składa się z zamkniętej mocnej ramy stalowej oraz ruchomych podpór, gdzie montuje się okno lub drzwi. Przykład urządzenia przedstawiono na rysunku 2. Wszystkie elementy łączące urządzenia, szczególnie połączenia narożne, powinny wytrzymać obciążenia próbne stosowane podczas badania. Do urządzenia badawczego zamocowany jest aplikator obciążenia wyposażony w suwak hydrauliczny (lub podobne urządzenie obciążające) odpowiedni do przyłożenia wymaganej siły próbnej – maks. 20 kN.

Do badań dostarczyć należy funkcjonujące kompletne okno lub drzwi z ościeżnicą i okuciami, które powinno być osadzone przez producenta w ramie zastępczej – prostopadle i pionowo, bez skręcenia lub wygięcia. Po zamontowaniu wyrobu w urządzeniu badawczym należy wprowadzić stan utwierdzenia lub zablokowania zadeklarowany przez producenta.

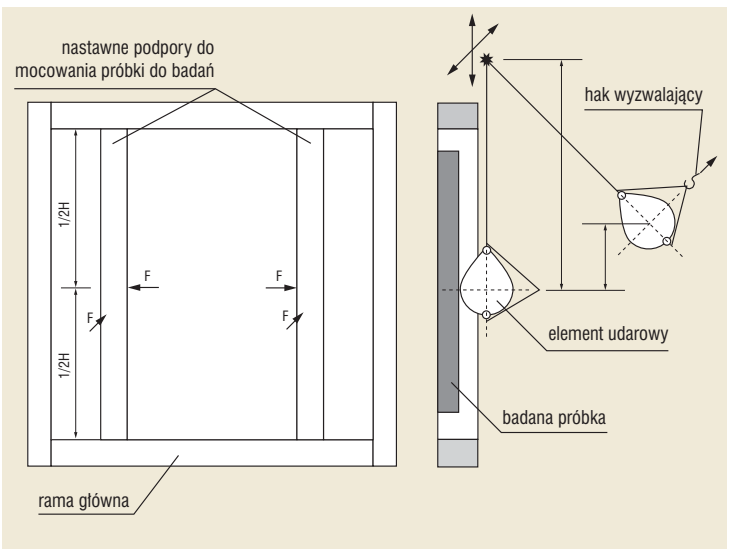
Określone obciążenia przykłada się do najsłabszych punktów badanej próbki z użyciem ustalonego aplikatora obciążeń. Obciążenie powinno być przykładane w równomiernym tempie, w czasie (60±5) s, od zera do wymaganego obciążenia. Po osiągnięciu maksymalnego obciążenia próbnego, które powinno być utrzymane przez (60±5) s, należy odczytać i zarejestrować odchylenie/ugięcie dla badania statycznego. Odciążanie powinno być dokonywane z tą samą prędkością.

Badanie odporności na obciążenie dynamiczne

Urządzenie badawcze składa się z zamkniętej mocnej ramy stalowej oraz ruchomych podpór, w które można



Rys. 2. Przykład urządzenia badawczego na obciążenie statyczne



Rys. 3. Przykład urządzenia badawczego na obciążenie dynamiczne

zamontować próbkę – okno lub drzwi do badań. Przykład urządzenia przedstawiono na rysunku 3. Wszystkie elementy łączące, szczególnie narożne, powinny wytrzymywać obciążenia próbne w trakcie badania. Do urządzenia badawczego przyłączony jest zespół udarowy składający się z worka skórzanego z piaskiem zawieszonego za pomocą odpowiedniej liny stalowej na ruchomej ramie, haka wyzwalającego (spustowego) i regulatora wysokości. Powstałe wahadło powinno mieć długość 1500 mm.

Próbka do badań dynamicznych powinna być przygotowana analogicznie jak do badań statycznych. Badanie dynamiczne symuluje fizyczny atak (bez użycia narzędzi), np. natarcie ramieniem, kopnięcie, i dlatego atakowane powinny być najsłabsze punkty badanej próbki.

Badanie polega na uniesieniu worka z hakiem na odpowiednią wysokość i następnie na rozłączeniu, co pozwala na swobodny ruch wahadłowy worka w kierunku badanej próbki. Należy to powtórzyć określoną ilość razy. Po każdym uderzeniu badana próbka powinna być skontrolowana pod kątem uszkodzeń.

Badanie odporności na próby włamania ręcznego

Urządzeniem badawczym jest stalowa rama jak do badania dynamicznego, w której osadza się funkcjonujące okno lub drzwi zamocowane w ramie zastępczej.

Badanie przeprowadza zespół składający się z osób zatrudnionych w laboratorium badawczym (kierownik, chronometrażysta i operator) i wyposażony w chronometr do mierzenia czasu oraz sprzęt pomiarowy do określenia temperatury i wilgotności drewna (przy badaniach wyrobów drewnianych).

W badaniach określa się następujące miejsca ataku:
- atak na części zamykające,
- atak na części ruchome,
- atak na bryłę próbki,
- atak na okucie,
- atak na wszelkie inne miejsca mające znaczenie.

Laboratorium badawcze przeprowadza w pierwszej kolejności badanie wstępne, którego celem jest ustalenie słabych miejsc okna lub drzwi. Podczas tych prób każde powyżej wskazane miejsce ataku jest badane przez co najmniej 25% czasu oporu wymaganego dla przewidywanej klasy. Na podstawie ustalonych w tych badaniach najsłabszych miejsc okna lub drzwi określa się ostateczny program badania głównego.

W badaniu głównym powinna być wykonana próba zmierzająca do siłowego otwarcia badanej próbki lub utworzenia otworu dostępu z użyciem określonego zestawu narzędzi w ramach czasu oporu i całkowitego czasu badania odpowiadającego danej klasie odporności według normy PN-ENV 1627:2006 (tab. 4). Od momentu rozpoczęcia badania głównego należy mierzyć czas oporu i całkowity czas badania. Dla wymiany narzędzi trwającej dłużej niż 5 s, np. w celu zastąpienia wadliwych narzędzi, pomiar czasu oporu powinien być przerywany.

Producent przy przekazywaniu do badań powinien określić stronę ataku, z zasady od strony zewnętrznej usytuowania okna lub drzwi w obiekcie, co należy odnotować w sprawozdaniu z badań.

Podczas badań operator może wybierać z danego zestawu narzędzi, właściwego dla przewidywanej klasy odporności.

W normie PN-ENV 1630:2006 określono następujące zestawy narzędzi:

Zestaw A
- 1 wkrętak o długości 260 mm i szerokości ostrza 10 mm,
- 1 wkrętak o długości 375 mm i szerokości ostrza 16 mm,
- kliny drewniane lub tworzywowe o długości 200 mm,
- 1 szczypce zaciskowe nastawne o długości 240 mm,
- 1 klucz do rur o długości 240 mm.

Zestaw B

narzędzia z zestawu A i dodatkowe:
- 1 łom stalowy o długości 710 mm,
- 1 wkrętak o długości 375 mm i szerokości ostrza 16 mm.

Zestaw C

narzędzia z zestawu B i dodatkowe:
- 1 młotek o długości 300 mm i maks. masie 1,25 kg,
- 1 siekierka o długości 350 mm,
- 1 szczypce przegubowe do prętów o długości 460 mm,
- 1 przecinak ślusarski o długości 250 mm i szerokości ostrza 30 mm,
- 1 dłuto ciesielskie płaskie o długości 350 mm i szerokości ostrza 30 mm,
- 1 piłka do metalu z brzeszczotami ze stali szybkotnącej,
- 1 wiertarka elektryczna o mocy 320/160 W,
- wiertła ze stali szybkotnącej o maksymalnej średnicy 10 mm,
- nożyce do blach grubych lewotnące i prawotnące o długości 160 mm.

Zestaw D

narzędzia z zestawu C i dodatkowe:
- 1 elektryczna piła – wyrzynarka o mocy 550/335W z brzeszczotami,
- 1 elektryczna piła bagnetowa o mocy 900/520W z brzeszczotami,
- 1 rura przedłużająca o maks. długości 500 mm,
- 1 wiertarka elektryczna o mocy 600/310 W,
- wiertła ze stali szybkotnącej lub węglików spiekanych o maks. średnicy 13 mm,
- rozwiertak rdzeniowy (koronka rdzeniowa) ze stali szybkotnącej lub węglików spiekanych o maks. średnicy 50 mm,
- 1 szlifierka kątowa o mocy 1000/575 W i maks. średnicy tarczy 125 mm.

Zestaw E

narzędzia z zestawu D i dodatkowe:
- 1 wiertarka elektryczna o mocy 1050/620 W,
- 1 szlifierka kątowa o mocy 1900/1175 W i maks. średnicy tarczy 230 mm.

W badaniach dla wszystkich klas odporności mogą być dodatkowo użyte drobne narzędzia, takie jak małe wkrętaki, nóż, klucze maszynowe i z gniazdem sześciokątnym, sznurek i drut stalowy, latarka i taśma przylepna oraz odzież ochronna (rękawice, okulary).

Po badaniach (również statycznych i dynamicznych) laboratorium sporządza sprawozdanie, które nie może być publikowane, nawet częściowo.

INŻ. ZBIGNIEW CZAJKA
INSTYTUT TECHNIKI BUDOWLANEJ
ODDZIAŁ WIELKOPOLSKI POZNAŃ

New Generation Security System

GANZ

Rejestrator DR16NRT-DVD

produced by CBC

Nowa generacja systemów CCTV, zaprojektowanych i wyprodukowanych przez CBC - światowego lidera na rynku CCTV gwarantującego niezrównaną jakość i niezawodność swoich produktów.

WORLD WIDE NETWORK

- Nagrywanie REAL TIME (400 klatek/sek.)
- Wysoka jakość XVGA wyświetlanego obrazu
- Inteligentny analizator obrazu do wyszukiwania nagrań
- Obsługa DDNS oraz synchronizacja czasu NTP
- 4 niezależne wyjścia SPOT z podziałem typu QUAD
- Obsługa 4 dysków wewnętrznych ATA/ESATA o pojemności 4x750GB

www.cbcpoland.pl

Systemy IP
z Pelco

Przejście od systemów analogowych CCTV do IP powoli staje się faktem. Celem artykułu jest pokazanie możliwości budowania małych i średnich systemów telewizji dozorowej IP na bazie kamer i rejestratorów produkowanych przez firmę Pelco

Wszystkie urządzenia kamerowe IP z firmy Pelco mają pewne cechy wspólne: stosowana jest kompresja MPEG4, maksymalna rozdzielczość to 4CIF, w wersjach z kodowaniem koloru w systemie PAL strumień wideo zawiera 25 obrazów/s. Wbudowany w każdą kamerę serwer wideo może wprowadzać do sieci trzy strumienie wideo. Dwa strumienie MPEG4 25 obrazów/s mogą być odbierane przez urządzenia odbiorcze, które obsługują protokół transmisji urządzeń IP Pelco. Jeden strumień jest używany do przesyłania danych do rejestratora w trybie „*unicast*". W tym trybie transmisja pakietów danych odbywa się z potwierdzeniem, co daje pewność, że wszystkie pakiety z materiałem wideo zostaną odebrane przez rejestrator. Drugi strumień może być przesłany do stacji roboczej, np. WS5060 w systemie Endura, w celu wyświetlenia obrazu ma monitorze. Odbywa się to w trybie „*multicast*". W tym trybie transmisja danych wideo odbywa się bez potwierdzenia, ale za to do wielu odbiorników jednocześnie – czyli do wszystkich stacji roboczych, które wyświetlają ten sam obraz.

Kamery IP Pelco obsługują protokoły: TCP/IP, UDP/IP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP i NTP. Urządzenia mogą pracować w czterech rozdzielczościach (PAL): 4CIF (704x576), 2CIF (704x288), CIF (352x288) i QCIF (176x144).

Trzeci strumień MJPEG, 15 obrazów/s, może być odbierany bezpośrednio przy użyciu przeglądarki internetowej Microsoft Internet Explorer lub Mozilla Firefox. Serwer wideo umożliwia jednoczesny odbiór strumieni wideo przez dziesięciu użytkowników korzystających z przeglądarek. Wymagane jest logowanie z hasłem. Użytkownik może oglądać wideo w trybie pełnoekranowym lub w oknie skalowalnym oraz przechwytywać i zapisywać pojedyncze obrazy do wydruku oraz przesłania e-mailem.

Do grupy firm, które współpracują z Pelco i opracowały sterowniki do kamer IP dla swoich produktów, należą m.in.: Milestone Systems, ObjectVideo, OnSSI, Plustek Inc., Visual Defence i Lenel Systems International Inc. Wszystkie kamery IP z Pelco mogą pracować w systemie dystrybucji wideo w sieciach IP Endura oraz z rejestratorem DVR5100 wersja 1.5. W momencie pisania tego artykułu trwały prace nad stworzeniem sterownika do obsługi Spectry IP dla rejestratora Integral Digital Sentry.

Kamery IP

Pelco produkuje dziewięć typów stacjonarnych kamer IP: osiem modeli kamer kopułkowych serii IP110 i jeden model w obudowie typu „box" IP3701-2X.

Kamery kopułkowe IP110 mogą być wyposażone w cztery rodzaje modułów kamerowych: kolorowy wysokiej rozdzielczości 540 TVL, dzienno-nocny wysokiej rozdzielczości 540 TVL, kolorowy z szerokim zakresem dynamiki oraz dzienno-nocny z szerokim zakresem dynamiki. Wersje WDR mogą pracować w trybie skanowania progresywnego. Dostępne są dwa obiektywy o regulowanej ogniskowej: 3,0–9,5 mm oraz 9,0–22,0 mm. Dodatkową funkcjonalność zapewnia wyjście alarmowe oraz parametryzowane wejście alarmowe. Obudowa o konstrukcji stalowo-aluminiowej jest przeznaczona do montażu wewnętrznego lub zewnętrznego (IP66) bezpośrednio na ścianie lub na suficie. Istnieje możliwość montażu na opcjonalnym uchwycie IP110-P. Kamera wymaga zasilania napięciem przemiennym 24 V z zewnętrznego zasilacza lub poprzez Ethernet w standardzie PoE. Zakres temperatur pracy urządzenia wynosi od -46°C do 50°C.

IP3701-2X to kamera kolorowa z przetwornikiem 1/3 cala o rozdzielczości 480 TVL. Do kamery można zastosować obiektyw o stałej lub regulowanej ogniskowej, na przykład z serii 13VD lub z korekcją IR serii 13VDIR. Minimalne oświetlenie to 0,5 luksa (lx) przy f1.2, 40 IRE i włączonym AGC. Kamera może być zainstalowana w obudowie wewnętrznej lub zewnętrznej z grzałką, na przykład z serii EH3512.

Systemy kamerowe IP PTZ

W lipcu firma Pelco wprowadziła do sprzedaży system kamerowy Spectra IV IP, kolejny wariant swojego docenianego na całym świecie produktu. Jest to dualny system kamerowy PTZ, który może pracować w instalacji analogowej i sieciowej IP. Spectra IV IP zawiera wszystkie rozbudowane funkcje analogowej Spectry IV, łącznie z analogowym wyjściem wideo i sterowaniem. Jednocześnie jest możliwe podłączenie do sieci IP i przesyłanie wideo i sterowania PTZ w postaci pakietów sieciowych.

Spectra IV IP jest dostępna w kilku wersjach obudowy: wewnętrznej do montażu wpuszczanego w suficie, wewnętrznej do montażu na wysięgniku, zewnętrznej do montażu w suficie, zewnętrznej do montażu na wysięgniku (IP66, zakres temp. od +50°C do -45°C) oraz w wykonaniu wzmocnionym i stalowym. Do obudów mogą być użyte opcjonalne uchwyty i adaptery do montażu na ścianie, słupie, dachu, w narożniku i do balustrady. Wybrane obudowy zawierają pamięć, w której przechowywane są ustawienia modułu kamerowego programowane przez instalatora. Po wymianie modułu kamerowego ustawienia są automatycznie przeładowywane z obudowy do nowego modułu.

W systemie Spectra mogą być stosowane moduły kamerowe w wersji dzień – noc o powiększeniach optycznych 35x, 23x i 18x oraz w wersji kolor 22x i 16x. Najbardziej zaawansowany technicznie jest moduł kamerowy z 35-krotnym powiększeniem. Może pracować w trybie progresywnego skanowania lub z przeplotem. Rozdzielczość lepsza niż 540 TVL zapewnia bardzo dobrą jakość obrazu. Kamera charakteryzuje się szerokim, 128-krotnym zakresem dynamiki. Czułość dla trybu czarno-białego wynosi 0,00018 lx przy migawce 1/1,5 s oraz 0,063 lx przy migawce 1/3 s w trybie kolorowym, pomiary przy poziomie wyjściowym 35 IRE. Kamera jest wyposażona w zintegrowany system elektronicznej stabilizacji i poprawy jakości obrazu oraz detekcji ruchu. Szybkość obrotu po wybraniu presetu wynosi 400°/s, a przy sterowaniu ręcznym w trybie Turbo – 150°/s.

Kopuły, tak jak w poprzednich modelach Spectry, mogą być przeźroczyste, przyciemnione, chromowane albo złocone. Występują w wersjach odpowiednich dla rodzaju zastosowanej obudowy.

Kolejnym produktem IP z Pelco będzie Spectra Mini IP – kamera obrotowa z dziesięciokrotnym powiększeniem optycznym przeznaczona do zastosowań wewnętrznych. Wprowadzenie do sprzedaży jest zapowiadane na czwarty kwartał 2008 roku.

Rejestratory

Rodzina rejestratorów Pelco DVR5100 z oprogramowaniem w wersji 1,5 to urządzenia hybrydowe. Każdy z trzech modeli może rejestrować wideo w 20 kanałach. DVR5104 rejestruje 4 sygnały analogowe + 16 IP, DVR5108: 8 analogowych + 12 IP i DVR5116: 16 analogowych + 4 IP. Maksymalna szybkość zapisu w trybie 4CIF dla rejestratora w wersji PAL wynosi 500 obrazów/s, co odpowiada 25 obrazom/s na kanał, czyli jest to zapis materiału w czasie rzeczywistym.

Rejestratory DVR5100 zawierają dwa dyski o łącznej pojemności nie przekraczającej 2 TB. W celu efektywnego zarządzania pojemnością dysków w DVR5100 zastosowano technologię EnduraStor pochodzącą z systemu Endura. Po

upłynięciu zadanego czasu od momentu zapisu materiału, na przykład 72 h, rejestrator ponownie przetwarza materiał zarejestrowany z szybkością 25 obrazów/s. Ze strumienia MPEG4 usuwane są klatki różnicowe i pozostają tylko klatki pełne, co daje w wyniku materiał zawierający 2 obrazy/s, składający się z pełnowartościowych klatek. Pozwala to zaoszczędzić około 50% powierzchni dyskowej.

Wybierając rejestrator serii DVR5100, użytkownik końcowy ma otwartą drogę rozbudowy swojego systemu CCTV do dużego systemu IP Endura. DVR5100 jest rejestrowany w systemie Endura jako jeden z rejestratorów systemowych, a materiał wideo może być wyświetlany na stacjach roboczych WS5060 i konsolach wyświetlania VCD5000.

W czwartym kwartale 2008 planowane jest wprowadzenie do oprogramowania DVR5100 funkcji łączenia rejestratorów w grupę. Pozwoli to między innymi na sterowanie z jednej klawiatury KBD5000 kamer PTZ podłączonych do maksimum pięciu rejestratorów.

Drugą rodziną rejestratorów Pelco, które obsługują kamery IP, są urządzenia Integral Digital Sentry NVR. Szczególną cechą tych rejestratorów jest możliwość obsługi kamer IP różnych producentów w jednym systemie, w tym także kamer megapikselowych. W przypadku zapisu strumieni wideo z kamer megapikselowych w rejestratorze zajmowany jest więcej niż jeden kanał. Modele 4- i 16-kanałowe nagrywają w trybie 4CIF (PAL) 25 obrazów/s, a model 32-kanałowy – 12,5 obrazów/s. Rejestratory DS NVR mogą być wyposażone w dyski o pojemności maksymalnej 1,5 TB. Dostępne są też zewnętrzne 3-, 6- i 18-terabajtowe macierze dyskowe RAID5. Istnieje możliwość zakupu samego oprogramowania DS NVs i zainstalowania go na własnym komputerze. Jeśli stworzony zostanie system telewizji dozorowej IP oparty na kilku urządzeniach DS NVR, to jego obsługa będzie bardzo prosta. Intuicyjne w użyciu oprogramowanie klienckie pozwala użytkownikowi oglądać obrazy z dowolnej kamery w wybranym podziale. Unikatową cechą systemów Integral Digital Sentry jest też głęboka integracja z systemem BMS Andover Continuum, umożliwiająca nadzór rejestratora oraz pobieranie wideo i komunikatów alarmowych.

Niniejszy artykuł nie zawiera szczegółów na temat systemu IP Endura, który jest przeznaczony do dużych i rozległych geograficznie instalacji telewizji dozorowej.

W Polsce produkty Pelco są dostępne w sieci Partnerów firmy TAC Sp. z o.o., 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

LG

Life's Good

Telewizja Przemysłowa

NOWOŚĆ

LS901P-B

- kamera Dzień/Noc
- wysoka rozdzielczość 570/700 linii
- czułość 0,00003 lux (Sens-Up)
- zdejmowany filtr IR
- HSBLC
- 3D-DNR
- procesor XDI
- zasilanie 12VDC/24VAC

NOWOŚĆ

LS902P-B

- kamera Dzień/Noc
- wysoka rozdzielczość 570/700 linii
- czułość 0,01 lux
- zdejmowany filtr IR
- WDR
- 3D-DNR
- procesor XDI
- zasilanie 12VDC/24VAC

NOWOŚĆ

LS903P-B

- kamera Dzień/Noc
- wysoka rozdzielczość 570/700 linii
- czułość 0,00003 lux (Sens-Up)
- zdejmowany filtr IR
- WDR & HSBLC
- 3D-DNR
- procesor XDI
- zasilanie 12VDC/24VAC

NOWOŚĆ

LE3116D

- rejestrator cyfrowy
- 400kl/sek
- kompresja MPEG4
- nagrywarka DVD
- karta sieciowa
- inteligentne wszukiwanie
- do 16 rejestratorów w systemie
- pojemność dysków do 3TB

LVC-SX811HP

- kamera Dzień/Noc
- wysoka rozdzielczość 500linii
- czułość 0,4/0,1lux
- zdejmowany filtr IR
- zasilanie 12VDC/24VAC

LPT-EP553PS

- kamera szybkoobrotowa Dzień/Noc
- wysoka rozdzielczość 520 linii
- czułość 1/0,005lux
- 27 x zoom optyczny
- zdejmowany filtr IR
- WDR, DSS, strefy prywatności
- uchwyt ścienny

Jedyny dystrybutor:

JANEX INTERNATIONAL

Profesjonalne Systemy Zabezpieczeń

Janex International Sp. z o.o.
ul. Płomyka 2 02-490 Warszawa
tel.: 022 863 63 53 fax: 022 863 74 23
e-mail: janex@janexint.com.pl www.janexint.com.pl

artykuł sponsorowany

Rejestrator dla małych systemów

NV-DVR1014

marki NOVUS

Zdecydowanie łatwiej jest przedstawiać zalety oraz wybrane funkcje rejestratorów zaawansowanych technicznie, posiadających wiele nowatorskich rozwiązań aniżeli rejestratorów ze średniej półki. Niemniej jednak to właśnie te rejestratory cieszą się największym zainteresowaniem klientów oraz dominują pod względem ilościowym sprzedaży. W popularnym segmencie rejestratorów czterokanałowych jest bardzo silna konkurencja, a parametry poszczególnych modeli i marek są bardzo podobne. Dlatego w tym kontekście warto zapoznać się z możliwościami technicznymi nowego czterokanałowego rejestratora marki NOVUS o nazwie NV-DVR1014

NV-DVR1014 pracuje w trybie triplex, umożliwiając równocześnie zapis, podgląd na żywo oraz połączenia sieciowe. W rejestratorze zastosowano efektywny system kompresji MPEG4 z czterema poziomami kompresji. Rejestrator może zapisywać do 100 obrazów na sekundę w rozdzielczości 360x288 i 25 obrazów na sekundę w rozdzielczości 720x288 dla wszystkich kamer. System operacyjny rejestratora oparto o Linux.

Rejestrator posiada przyjazne dla użytkownika wielopoziomowe graficzne menu wyświetlane na ekranie monitora, służące do programowania ustawień i egzekwowania funkcji, takich jak odtwarzanie czy kopiowanie. Menu wyświetlane jest w pięciu językach, między innymi w języku polskim.

Nagrywanie obrazów z kamer może być realizowane w następujących trybach: ręcznym ze zdefiniowanymi prędkościami, ciągłym i alarmowym oraz w jednym z pięciu dostępnych harmonogramów. W ramach harmonogramu dla każdego dnia tygodnia z rozdzielczością jednej godziny można zdefiniować tryby nagrywania ciągłego albo alarmowego lub wybrać brak nagrywania.

W rejestratorze nagrywanie alarmowe obejmuje zdarzenia wywołane zarówno detekcją ruchu, jak i aktywacją wejść alarmowych.

Rejestrator wyróżnia się różnorodnością sposobów jego obsługi. Może być ona realizowana z poziomów poziomu przycisków panelu czołowego, za pomocą pilota sterowania zdalnego o zasięgu do siedmiu metrów, myszy USB znajdującej się w zestawie oraz z poziomu klawiatur systemowych NV-KBD60 oraz NV-KBD30 przy użyciu protokołu D2.

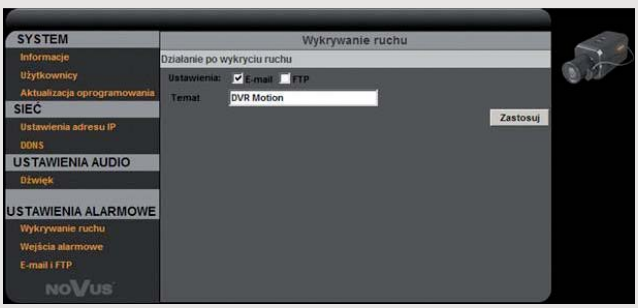
Rejestrator NV-DVR1014 pozwala sterować czterema kamerami wyposażonymi w interfejs RS485. Mogą to być zarówno kamery szybkoobrotowe serii CAMA-I, CAMA-II oraz CAMA-II mini, jak i stacjonarne z optycznym i cyfrowym zbliżeniem. Sterowanie może być realizowane z poziomu przycisków na płycie czołowej, za pomocą myszy USB z poziomu menu ekranowego lub z poziomu oprogramowania sieciowego. Sterowanie odbywa się zgodnie z protokołem Novus-C, Novus-C1, Novus-C2 lub Pelco-D, z możliwością regulacji prędkości uchyłu i obrotu. Rejestrator umożliwia zdefiniowanie parametrów transmisji oddzielnie dla każdej kamery, tym samym w systemie można równocześnie sterować kamerami w różnych protokołach.

W rejestratorze można zainstalować jeden wewnętrzny dysk twardy o maksymalnej pojemności 500 GB. Płyta główna rejestratora została wyposażona w kontrolery dysku twardego SATA, co jest ważne w kontekście wycofywania się producentów dysków z równoległego interfejsu komunikacyjnego PATA. Informacja ta jest szczególnie istotna w przypadku wieloletniej eksploatacji rejestratora, którego dyski twarde są najsłabszym ogniwem i w trakcie użytkowania systemu należy uwzględnić ich wymianę. Dysk w rejestratorze pracuje nieprzerwanie przez cały czas eksploatacji systemu.

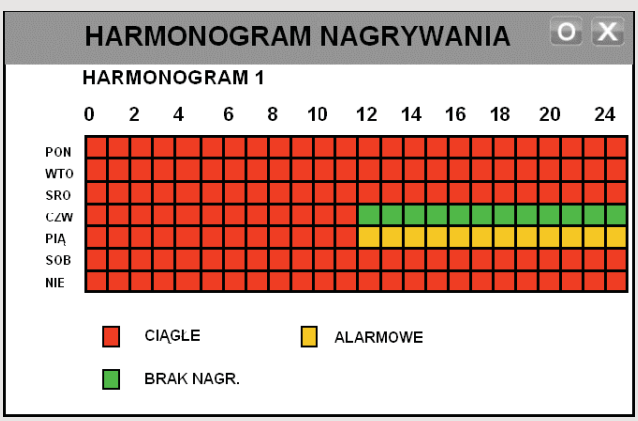
Rejestrator posiada jedno wyjście monitorowe główne z interfejsami BNC oraz VGA, które mogą pracować równocześnie. Wyposażenie rejestratora w interfejs VGA jest szczególnie użyteczne w niskobudżetowych systemach nadzoru wizyjnego, ponieważ pozwala na użycie do zobrazowania informacji standardowych i powszechnie dostępnych (w przeciwieństwie do typowych analogowych monitorów CCTV) monitorów komputerowych.

Rejestrator ma jedno wejście audio (mikrofonowe) oraz jedno wyjście głośnikowe. Do rejestrowanej ścieżki dźwiękowej użytkownik ma dostęp nie tylko lokalnie, ale również zdalnie poprzez sieć komputerową (odsłuch na żywo i odtwarzanie). Co ważniejsze, przy kopiowaniu strumienia wideo zapisywana jest również ścieżka audio.

Fot. 1. Graficzne menu główne rejestratora



Fot. 2. Ustawienia wysyłania obrazów na adres e-mail lub serwer FTP w przypadku detekcji ruchu



Fot. 3. Menu ustawień harmonogramu nagrywania

Fot. 4. Wygląd interfejsu sieciowego rejestratora

W rejestratorze zaimplementowano możliwość wyłączenia wyświetlania obrazu z kamer na monitorze głównym. Nie powoduje to jednak zatrzymania nagrywania. Pozwala to na rejestrację obrazów z tych kamer, dla których obserwacja obrazu przez operatorów jest niedozwolona. Dodatkowo można ograniczyć dostęp do trybu odtwarzania poprzez zablokowanie przycisków panelu czołowego za wyjątkiem przycisków podziału i „MENU". Dostęp do menu rejestratora wymaga autoryzacji hasłem. Tak zaplanowany system pozwala chronić zarejestrowane dane oraz ustawienia przed nieautoryzowanymi próbami ich zmiany.

Urządzenie ma cztery definiowane w menu wejścia alarmowe (NO lub NC), jedno wyjście alarmowe oraz wewnętrzny brzęczyk. W przypadku aktywacji wejścia alarmowego, detekcji ruchu dla wybranego kanału albo utraty sygnału może być uaktywniany brzęczyk lub wyjście alarmowe. Ponadto nastąpi pełnoekranowe wyświetlenie obrazu z powiązanej ze zdarzeniem kamery na monitorze głównym. Wszystkie te zdarzenia mogą być zapisywane w rejestrze systemowym o pojemności 3000 zdarzeń i powiązane z nagranym materiałem.

Rejestrator umożliwia pracę w sieci komputerowej, wykorzystując protokół TCP/IP. Połączenie jest realizowane z poziomu przeglądarki Internet Explorer. Możliwych jest pięć równoczesnych połączeń z rejestratorem w trybie na żywo oraz jedno w trybie odtwarzania.

Dostęp zdalny do zasobów rejestratora wymaga autoryzacji niezależnym hasłem sieciowym.

Podczas przeglądania obrazów w trybie na żywo oraz odtwarzania jest możliwość zapisania interesującego fragmentu w postaci pliku AVI.

W menu interfejsu sieciowego można dokonać ustawień dotyczących wysyłania obrazów na serwer FTP i e-maili. Po wykryciu ruchu lub w momencie wysterowania wejścia alarmowego rejestrator wysyła e-mail z załączonym obrazem lub eksportuje obraz na serwer FTP. Funkcja ta pozwala na szybki zdalny dostęp do zdarzeń alarmowych w systemie oraz uzyskanie zdalnej kopii zdarzeń alarmowych, ważnych szczególnie w przypadku utraty lub fizycznego zniszczenia rejestratora.

Rejestrator NV-DVR1014 posiada możliwość kopiowania zarejestrowanych na dysku twardym danych na pamięci Flash z interfejsem USB. Razem z plikiem kopii na pamięć kopiowany jest program F4Viewer.exe, za pomocą którego możliwe jest przeglądanie na komputerze PC pliku kopii. Odtwarzacz posiada dodatkowo funkcję przeglądania zawartości dysków z nagraniami wyjętych bezpośrednio z rejestratora. Jest to szczególnie ważne w przypadku konieczności przeanalizowania nagrań z dłuższego okresu, których kopiowanie byłoby procesem długotrwałym. Oglądane nagrania można zapisać na komputerze PC, a następnie skonwertować do pliku AVI.

Rejestrator jest ciągle rozwijany i uzupełniany o dodatkowe funkcje. Aktualizacja oprogramowania wbudowanego w sprzęt (ang. *firmware*) przez użytkowników systemu pozwala na rozszerzanie funkcjonalności już pracujących systemów zgodnie z aktualnym stanem. Trwają również prace nad umożliwieniem dostępu do jego zasobów poprzez coraz popularniejsze urządzenia mobilne.

Patryk Gańko
NOVUS

NOVUS®

Profesjonalne rozwiązanie dla systemów CCTV

NOWA generacja rejestratorów

4-kanałowy rejestrator cyfrowy serii 1000

- tripleks: zapis, odtwarzanie i połączenia sieciowe
- prędkość nagrywania do 100 obr/s
- MPEG-4, rozdzielczość nagrywania: 720x288, 360x288
- możliwość zapisu 1 kanału audio
- harmonogram nagrywania
- detekcja ruchu z definiowanymi obszarami aktywnymi
- sterowanie kamerami PTZ
- kopiowanie nagrań poprzez sieć komputerową lub port USB
- w zestawie pilot zdalnego sterowania

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

artykuł sponsorowany

Nowe czujki zewnętrzne serii HX

Jedną z nowości firmy Optex zaprezentowanych na tegorocznych targach IFSEC są pasywne czujki podczerwieni (PCP) serii HX. Będące rezultatem wielu badań i innowacji urządzenia stanowią wyzwanie dla branży zabezpieczeń w zakresie detekcji intruza z wykorzystaniem pasywnej technologii podczerwieni

Produkując czujki ochrony zewnętrznej i od wielu lat zbierając doświadczenia w zakresie ich różnorakich zastosowań, firma Optex wypracowała szeroką i przekrojową ofertę takich urządzeń. Należą do niej znane instalatorom na całym świecie czujki serii LX, VX oraz BX, których już drugie generacje znajdują się na rynku od wielu lat. Walory użytkowe oraz uznanie dla jakości mierzonej pewnością detekcji i wieloletnim, bezawaryjnym użytkowaniem stanowiły punkt wyjścia do prac nad nowymi produktami. Dzięki wymianie informacji nieprzerwanie prowadzonej z klientami od wielu lat i dotyczącej mocnych i słabych stron istniejących produktów ustalono najistotniejsze parametry dla oceny użyteczności czujek. Pozwoliło to prowadzić badania nad nowymi technologiami detekcji i analizą sygnałów w taki sposób, aby uzyskać maksymalnie pewną detekcję intruza oraz wprowadzić udoskonalenia funkcjonalne wychodzące naprzeciw oczekiwaniom instalatorów i użytkowników. Dzięki temu firma Optex proponuje zupełnie nową konstrukcję – serię czujek HX, w których wszystko, zaczynając od piroelementu i soczewki, poprzez algorytmy przetwarzania, a na obudowie kończąc, zaprojektowano od początku.

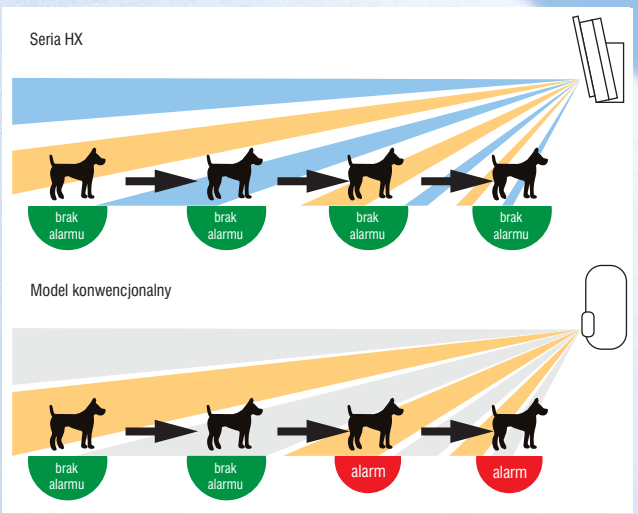
Nowe technologie

Projektując system optyczny dla nowej czujki, zwrócono szczególną uwagę na zachowanie tych samych parametrów detekcji na krańcach zasięgu, jak w pobliżu czujki. To bardzo trudne zadanie, zważywszy na efekt perspektywy. Powstała więc technologia Wielowarstwowego Pokrycia Pola Detekcji (ang. *Multiple Pattern Detection Area Technology*). Istotą tej technologii jest naprzemienne ułożenie warstw pól detekcji pochodzących z dwóch niezależnych torów PCP w taki sposób, aby został zachowany stały odstęp pomiędzy poszczególnymi warstwami. Wymagało to zaprojektowania bardzo precyzyjnego układu optycznego oraz zupełnie nowego piroelementu, które razem tworzą strukturę 94 pól detekcji o jednakowej gęstości zarówno w pobliżu detektora, jak i na krańcach jego nominalnego zasięgu. Takie podejście pozwala z jednakową pewnością odróżniać obiekty wielkości człowieka od innych, które mogą znaleźć się w polu widzenia czujki.

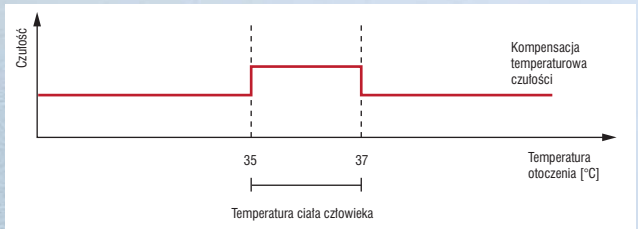
Nowy system optyczny wymaga również zupełnie nowego podejścia do analizy sygnałów pochodzących z dwóch kanałów PCP. Do identyfikacji intruza wykorzystano skomplikowaną analizę czasową aktywacji obu kanałów PCP, uwzględniającą wielkość sygnału (pośrednio również wielkość obiektu) oraz prędkość poruszania się. Inteligentny Iloczyn Logiczny (ang. *Intelligent AND Logic*) wraz z unikatowym systemem optycznym o 94 polach detekcji umożliwia niezawodną identyfikację intruza oraz ignorowanie małych zwierząt (o wysokości ok. 50 cm i masie ok. 10 kg) operujących w polu widzenia czujki.

Jedną z najważniejszych nowinek technologicznych czujek HX jest układ dualnej analizy sygnałów (ang. *Dual Signal Processing Circuit*), który odpowiada za kompensację temperatury otoczenia. Potrzeba kompensacji temperatury jest oczywista i wynika z zasady działania PCP – wykorzystania różnicy emitowanego promieniowania podczerwonego pomiędzy tłem a poruszającym się intruzem. W sytuacji, w której temperatura otoczenia osiąga wartość zbliżoną do temperatury ciała człowieka, detekcja jest utrudniona, ponieważ zredukowany zostaje kontrast pomiędzy intruzem a tłem. Wówczas należy skorygować czułość detektora tak, aby umożliwić detekcję. W obrębie temperatur 35°C i 39°C czułość detektora powinna być co najmniej o 20% wyższa niż przy temperaturze 25°C. W ten sposób funkcjonuje większość zaawansowanych algorytmów kompensacji temperaturowej, w tym również algorytm firmy Optex.

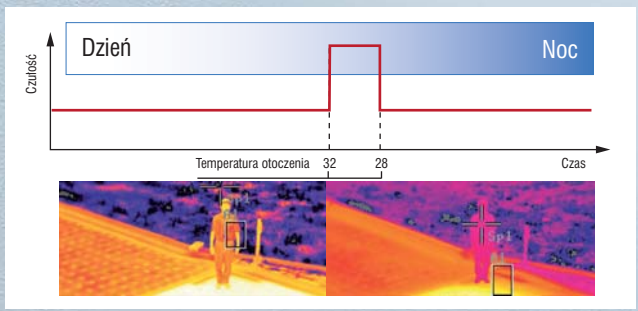
Jedną z największych bolączek detektorów zewnętrznych było ograniczenie zdolności detekcji intruza wieczorami po upalnych dniach. Wszelkie dotychczasowe algorytmy dobrze radzące sobie z detekcją w podwyższonych temperaturach pozostawały bezsilne w sytuacji, gdy temperatura otoczenia malała i kontrast pomiędzy intruzem a rozgrzanym tłem pozostawał bardzo mały (np. w temperaturze 20°C człowiek może być niewidoczny na tle chodnika czy ściany budynku nagrzanej do 37°C w ciągu dnia). Rozwiązaniem tego nader istotnego problemu jest algorytm *Summer Night Compensation Logic*, który analizując zmiany temperatury, wprowadza niezbędne korekty do ustawień czułości detektora. W najprostszy sposób można je opisać jako wydłużenie czasu, w którym detektor pracuje z wyższą czułością w zależności od warunków w ciągu dnia (czasu występowania wysokiej temperatury). Układ Dualnej Analizy Sygnałów zawiera oba algorytmy kompensacji temperaturowej, dając



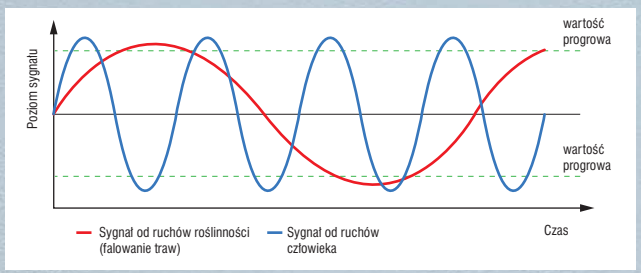
Rys. 1. Technologia Wielowarstwowego Pokrycia Pola Detekcji



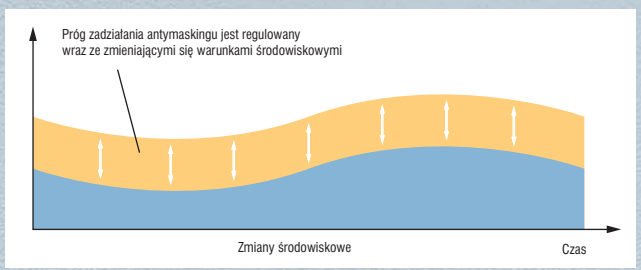
Rys. 2. Zaawansowana Kompensacja Temperaturowa



Rys. 3. Przykład działania algorytmu Summer Night Compensation



Rys. 4. Ilustracja zasady działania algorytmu Vegetation Sway Analysis



Rys. 5. Zasada działania cyfrowego algorytmu antymaskingu

czujce HX wyraźną przewagę w dziedzinie automatycznego dostosowania parametrów detekcji do panujących warunków otoczenia.

Na szczególną uwagę zasługuje również algorytm *Vegetation Sway Analysis Logic*. Analizie poddawany jest sygnał z obu kanałów PCP w celu identyfikacji oscylacyjnych pobudzeń charakterystycznych dla roślinności znajdującej się w polu widzenia czujki (traw, niewielkich krzewów itp.). Wykrycie takich zakłóceń spowoduje kompensację niepożądanego składnika sygnału, co poprawia dokładność dalszej obróbki sygnałów przez algorytmy identyfikacji intruza. Tego typu rozwiązanie, znane i stosowane dotychczas w czujkach mikrofalowych, zostało po raz pierwszy wprowadzone do czujek PCP. Jak potwierdzają nasze testy – z dużym sukcesem.

Funkcjonalność

Profesjonaliści branży zabezpieczeń często zwracają uwagę na stosunkowo niewielkie środki identyfikacji sabotażu czujek zewnętrznych. Zwłaszcza, że na zewnątrz są one daleko bardziej narażone na tego typu działanie. Dlatego czujki HX wyposażono w uchwyt montażowy z zamkniętym kanałem na okablowanie (dostarczany razem z czujką). Jeśli oczekujemy jeszcze wyższego stopnia ochrony, seria detektorów posiada model wyposażony w układ optycznego antymaskingu wykonany z wykorzystaniem tych samych technologii, co w serii OPTiMAL opisanej w poprzednim numerze czasopisma *Zabezpieczenia*. Firma Optex planuje również wprowadzenie na rynek dualnej czujki HX z dodatkowym kanałem mikrofalowym i wspomnianym optycznym układem antymaskingu.

Soczewka czujki ma budowę sektorową, dzięki czemu – stosując naklejki maskujące – można w łatwy sposób wyłączyć część jej pola widzenia. Przy tak skomplikowanym algorytmie detekcji również ograniczenie zasięgu dokonuje się skokowo, przez przesłonięcie odpowiednich fragmentów soczewki. Odpowiednio przygotowane naklejki ze specjalnego przezroczystego tworzywa są dostarczane w zestawie razem z czujką.

Modułowa budowa czujki ułatwia montaż, a rozmieszczenie zacisków i przełączników konfiguracyjnych jest bardzo wygodne dla instalatora, zapewnia bowiem szybki montaż okablowania i łatwy dostęp do wszystkich przełączników. Dbałość o jakość pracy instalatorów jest charakterystyczna dla wszystkich produktów firmy Optex.

Podsumowanie

Urządzenia zewnętrzne to znacząca pozycja w ofercie firmy Optex. Seria czujek HX, zaprezentowana po raz pierwszy na targach IFSEC'2008, jest jej istotnym wzmocnieniem. Jako produkt o bardzo wysokim zaangażowaniu nowych technologii, który stanowi wyraźny przełom w dziedzinie zewnętrznych PCP, umacnia pozycję firmy jako lidera systemów detekcji intruza. Oferowane rozwiązania wychodzą naprzeciw oczekiwaniom klientów i instalatorów. Są one owocem prowadzonych stale prac badawczych nad udoskonaleniem produktów oraz wykorzystaniem możliwości nowych technologii. Takie działanie jest istotą firmy Optex.

Jarosław Gibas
Optex Security

ELKRON

urmet MIWI

NOWE BARIERY PODCZERWIENI ELKRON

OPTYMALNA OCHRONA :

4 częstotliwości działania do wyboru, łatwa i szybka instalacja

EL50RT4PH-250m - 4 wiązki, zasięg wew. 500m / zew. 250m
EL50RT2PH-150m - 2 wiązki, zasięg wew. 300m / zew. 150m
EL50RT2PH-60m - 2 wiązki, zasięg wew. 120m / zew. 60m

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

Nowe technologie w ochronie infrastruktury krytycznej

Metodyka ochrony obiektów i organizacja systemów ochrony podlegają ciągłemu doskonaleniu w miarę rozwoju technologii i wprowadzania na rynek doskonalszych urządzeń. Stymulacja rozwoju nowych technologii wynika z potrzeby ciągłego „uszczelniania" ochrony obiektów publicznie dostępnych, a jednocześnie szczególnie ważnych w organizacji życia społecznego. Ogólnie nazywamy je obiektami szczególnego znaczenia objętymi obowiązkiem ochrony lub obiektami infrastruktury krytycznej (od ang.: *Critical Infrastructure*).

1. Wstęp

Do infrastruktury krytycznej zaliczamy rozległy wachlarz obiektów o zróżnicowanej strukturze użyteczności społecznej, np.:

- obiekty przemysłowe: rafinerie, elektrownie, zakłady produkcji chemicznej, zakłady produkcji uzbrojenia itp.,
- obiekty środków transportu: porty lotnicze, morskie, lądowe, samoloty, statki, pociągi, autobusy, tramwaje,
- magazyny, zbiorniki i infrastrukturę zaopatrzenia ludności w żywność, wodę, „powietrze" oraz energię,
- obiekty związane z bezpieczeństwem miast, zgromadzeń, imprez sportowych.

Obiekty infrastruktury krytycznej są zróżnicowane pod względem obszaru, budowy, rodzaju zagrożeń i ewentualnych skutków ataków przestępczych.

Niemniej jednak wszystkie wyżej wymienione obiekty można podporządkować pod unijny (europejski) model ochrony, wprowadzony przez Advisory Group of Security w 2005 r., który rozważa zabezpieczenie obiektów w trzech wymiarach: celu, zagrożenia i przeciwdziałania (*targets, threats and countermeasures*).

Celem i zadaniem zabezpieczenia każdego chronionego obiektu jest przeciwdziałanie możliwym zagrożeniom i uniemożliwienie wyrządzenia szkód, w tym poszkodowania osób, spowodowania strat materialnych czy zakłócenia funkcjonowania obiektu.

Zgodnie ze wspomnianym wcześniej modelem ochrony przeciwdziałanie to:

- integracja działania systemów ochrony technicznej (wyposażenia),
- integracja działania ludzi (obsługa systemów, interwencja fizyczna),
- organizacja zarządzania bezpieczeństwem i procedury postępowania.

W pełnym opisie organizacji przeciwdziałania, czyli zabezpieczenia obiektu, należałoby przedstawić problemy trzech wymienionych podsystemów organizacji zabezpieczeń. Z uwagi na techniczny charakter publikacji rozpatrzony zostanie tylko rozwój technologii urządzeń ze wskazaniem na tendencje rozwojowe systemów ochrony z zastosowaniem urządzeń nowych technologii. Ogólnie biorąc, system ochrony technicznej obiektu infrastruktury krytycznej można rozważać jako współdziałanie trzech systemów:

1. Systemu ochrony obwodowej (perymetrycznej) i otwartego obszaru obiektu;
2. Systemu ochrony mienia i kontroli ruchu osób w obrębie zabudowy obiektu;
3. Systemu monitoringu wizyjnego ogólnie dostępnych obiektów miast, stadionów, dworców, terminali lotniczych, obiektów handlowych, hal produkcyjnych itp.

Zakres zastosowania i rozbudowy danego systemu zależy od rodzaju rozważanego obiektu. Niemniej jednak technologie, na które zwrócona zostanie uwaga, mogą występować w różnych aplikacjach we wszystkich wymienionych wyżej systemach.

Dla właściwego zobrazowania postępu technologicznego przeciwstawione zostaną elementy systemu klasycznego i aktualnie wdrażanego.

1. W systemach ochrony perymetrycznej występuje w tym przeciwstawieniu klasyczny system uzbrojonej obwodnicy (ogrodzenie, systemy detekcji wzdłuż

obwodu obiektu oraz obserwacja kamerowa) i nowoczesny system radarowo-termowizyjny detekcji granicy ogrodzenia, obszaru otwartego i śledzenia intruza.

2. Klasycznej obserwacji wizyjnej z operatorem analizującym obrazy z kilkunastu kamer przeciwstawiamy „inteligentną" komputerową analizę obrazów termowizyjnych z automatycznym wskazaniem zaprogramowanej sceny będącej celem obserwacji.
3. Zamiast oddzielnej obserwacji ekranów wizualizacji wskazań radaru, kamer termowizyjnej i wizyjnej – fuzje na jednym ekranie ze zobrazowaniem i wskazaniem ruchu śledzonego obiektu i jego lokalizacji na mapie.
4. Zamiast dedykowanej wewnątrzsystemowej telekomunikacji – otwarte sieciowe systemy teleinformatyczne.

Poszczególne rozdziały artykułu będą poświęcone omówieniu wyżej wymienionych zagadnień.

2. System ochrony perymetrycznej nowej generacji

Na rys. 1 przedstawiono budowę klasycznej obwodnicy w systemie ochrony perymetrycznej.

Systemy tego rodzaju rozwijały się głównie w celu ochrony obiektów wojskowych składnic i baz jako obiektów oddalonych od terenów zabudowanych i chronionych przez wydzielone oddziały wartownicze. Główne elementy systemu stanowiły: podwójne ogrodzenie (zewnętrzne i wewnętrzne), podwójny system detekcji (podsystemy dwóch różnych technologii) i (albo zamiast jednego z systemów detekcji) wizualna weryfikacja alarmu z oświetleniem całej obwodnicy.

Koniecznym elementem takiego systemu jest kanalizacja rurowa do ułożenia kabli sygnałowych, wizyjnych i zasilania elektrycznego. Strefowy system zasięgu czujników, barier i kamer rzędu 100 m i oświetlenia (50 m) przy wielokilometrowym obwodzie chronionego obiektu rozrasta się do kilkudziesięciu elementów jednego podsystemu. Przy dwóch, trzech podsystemach obwodnicy liczba elementów (czujników ogrodzeniowych, barier naziemnych, kamer) sięga rzędu stu i więcej, co z kolei powoduje generowanie fałszywych alarmów w liczbie, która czyni system uciążliwym i mało skutecznym w codziennej eksploatacji. Zwłaszcza doświadczenia wieloletniej eksploatacji takich systemów przy słabej obsłudze serwisowej nie są zachęcające.

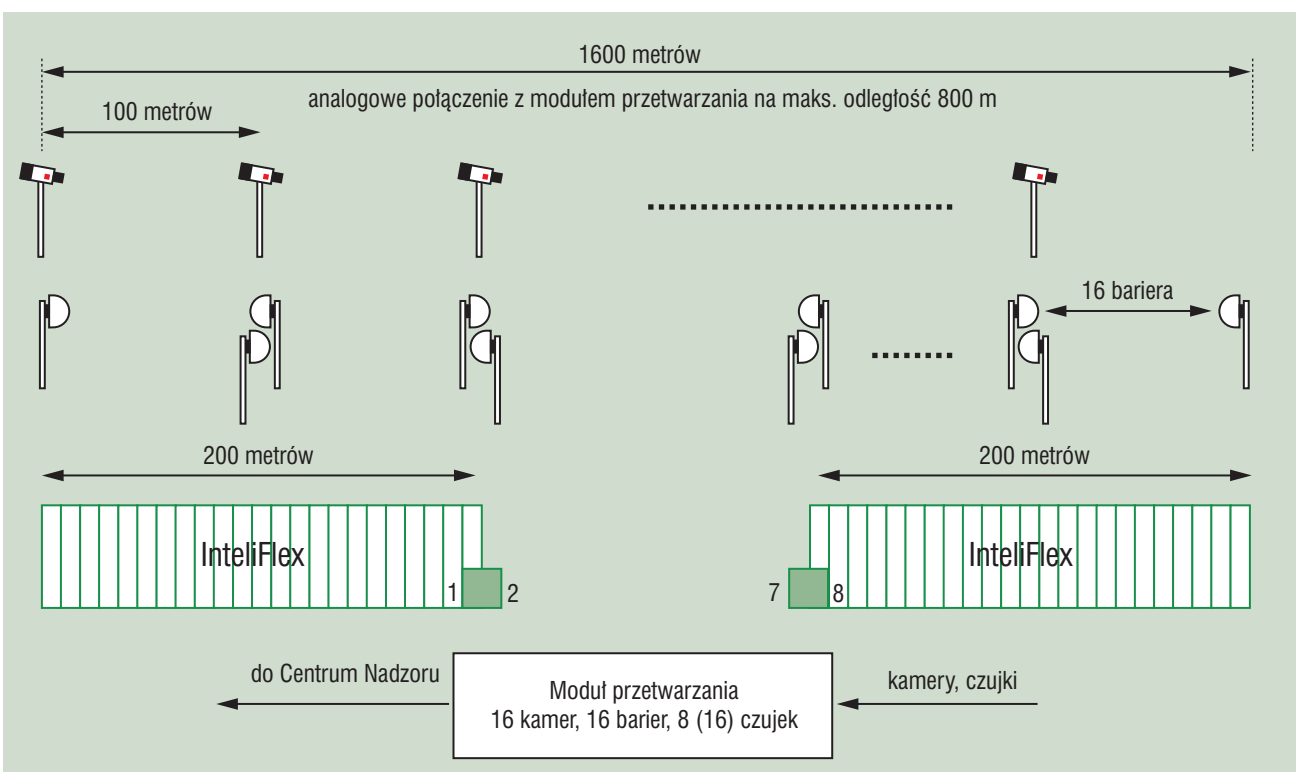
Poza wyżej wymienionymi problemami dowolny system ochrony perymetrycznej wykrywa naruszenie strefy tylko w wąskim pasie obwodnicy. Po przeniknięciu intruza przez pas chroniony ślad po nieproszonym gościu ginie, jako że teren między obiektem chronionym a obwodnicą nie jest monitorowany.

Patrol ochrony wyruszający na poszukiwanie intruza w kilku- lub kilkunastohektarowym terenie (często zalesionym) jest bardziej narażony na atak ze strony intruza niż poszukiwany intruz na ujawnienie.

W ciągu ostatniej dekady cele i zadania ochrony perymetrycznej uległy istotnej zmianie. Przebywanie wojsk wielu krajów w Afganistanie, Iraku, w zamkniętych, chronionych murem obozach, wytworzyło zapotrzebowanie na środki ochrony perymetrycznej z możliwością obserwacji poza ogrodzonym terenem obozu oraz możliwością wykrycia, rozpoznania, identyfikacji i śledzenia intruza bez względu na porę dnia i warunki atmosferyczne.

W krajach wysoko rozwiniętych, głównie w Ameryce i Europie, ochroną perymetryczną zostają objęte lotniska, elektrownie atomowe, fabryki chemiczne jako obiekty szczególnie narażone na ataki terrorystyczne.

W Polsce rozwija się grupa lotnisk regionalnych, które bazują głównie na byłych lotniskach wojskowych, oddalonych od aglomeracji miejskich, łatwo dostępnych ze skrytego podejścia do rozległego terenu. Typowy obwód tych lotnisk wynosi 12–15 km i obejmuje powierzchnię rzędu kilkuset hektarów. Tego rodzaju lotniska aktualnie poddaje



Rys. 1. Przykładowy klasyczny system ochrony perymetrycznej

się ochronie perymetrycznej. Z tego względu przyjmiemy typowe lotnisko jako przykładowy obiekt budowy ochrony perymetrycznej w nowej technologii.

Zgodnie z Zarządzeniem Urzędu Lotnictwa Cywilnego (ULC) realizującego zalecenia unijne ochrona lotnisk ma być zróżnicowana odnośnie środków i szczelności ochrony w zależności od strefy lotniska. Zarządzenie wyróżnia strefy – ogólnodostępną, zastrzeżoną, sterylną – i obiekty szczególnego znaczenia, takie jak płyta postojowa i obsługi statków powietrznych, wieża kontrolna, urządzenia naprowadzania do lądowania, magazyn paliw, stacje zasilania itp.

Ze względu na ochronę perymetryczną interesuje nas strefa zastrzeżona, która obejmuje cały teren lotniska objęty ogrodzeniem zewnętrznym. Zgodnie z zaleceniem ULC detekcja intruza ma nastąpić przy przekraczaniu ogrodzenia, ale wskazana jest obserwacja przedpola poza ogrodzeniem i śledzenie wykrytego intruza po przekroczeniu ogrodzenia na całym terenie otwartym lotniska oraz monitorowanie terenu lotniska, w tym pasa startowego i dróg kołowania.

A zatem ochrona rozległego obiektu infrastruktury krytycznej to nie tylko detekcja w pasie obwodnicy i odpowiedź na pytanie, czy intruz przekroczył obwodnicę czy nie, ale jeśli przekroczył, to także jego śledzenie i ciągłe przekazywanie jego obrazu oraz trasy ruchu patrolowi interwencji fizycznej. Zatem patrol interweniujący ma istotną przewagę taktyczną nad ewentualnym przeciwnikiem i szansę skutecznej interwencji.

Jak z tego wynika, funkcje ochrony obwodowej obiektów infrastruktury krytycznej w rozumieniu wytycznych unijnych uległy istotnemu rozszerzeniu. Tych wymagań ochrony nie spełni już żaden system w klasycznej organizacji w ramach obwodnicy jak na rys. 1. Niezbędne są bierne i aktywne systemy falowe, takie jak radary naziemne, kamery termowizyjne, kamery wizyjne, o zasięgach kilkusetmetrowych, wzajemnie sprzężone i wykrywające przekraczanie ogrodzenia oraz monitorujące w systemie okrężnym cały teren lotniska jako strefę zastrzeżoną. Rosną również wymagania względem Centrum Nadzoru w zakresie współpracy z załogą patrolu. Konieczne jest odwzorowanie terenu lotniska wraz z obiektami na mapie cyfrowej, lokalizacji intruza oraz patrolu we współrzędnych mapy i dynamiczne śledzenie wizyjne rozwoju wydarzeń w przypadku organizacji interwencji fizycznej.

Elementy współczesnego systemu ochrony rozległego obiektu infrastruktury krytycznej na przykładzie portu lotniczego zostały przedstawione na rys. 2.

Ogrodzenie aktywne, np. z czujnikiem światłowodowym z liniową detekcją miejsca zaburzenia, wyznacza granice strefy zastrzeżonej. Radar naziemny, kamera termowizyjna i kamera wizyjna mogą być montowane na jednej platformie lub oddzielnie sprzężone poprzez oprogramowanie Centrum Nadzoru. Radar o zasięgu rzędu 1200–1500 m obejmuje sektor ogrodzenia rzędu 2–3 km, posiada zdolność detekcji intruza odpowiednio do 800–1000 m i sięga „wzrokiem” poza ogrodzenie. Kamera termowizyjna i wizyjna ze sterowanym obiektywem (zoom) i z detekcją intruza na granicy ogrodzenia obserwuje wydzielony sektor. W przypadku wykrycia intruza przekraczającego ogrodzenie radar przejmuje sterowanie zespołem kamer i łącznie śledzą, rozpoznają i identyfikują intruza.

Centrum Nadzoru alarmuje patrol Służby Ochrony Lotniska (SOL), przekazuje wizyjnie obraz intruza i jego położenie na mapie lotniska i śledzi rozwój wydarzeń. Patrol lokalizuje swoje położenie za pomocą GPS i rejestruje swój ruch na mapie własnej i Centrum Nadzoru.

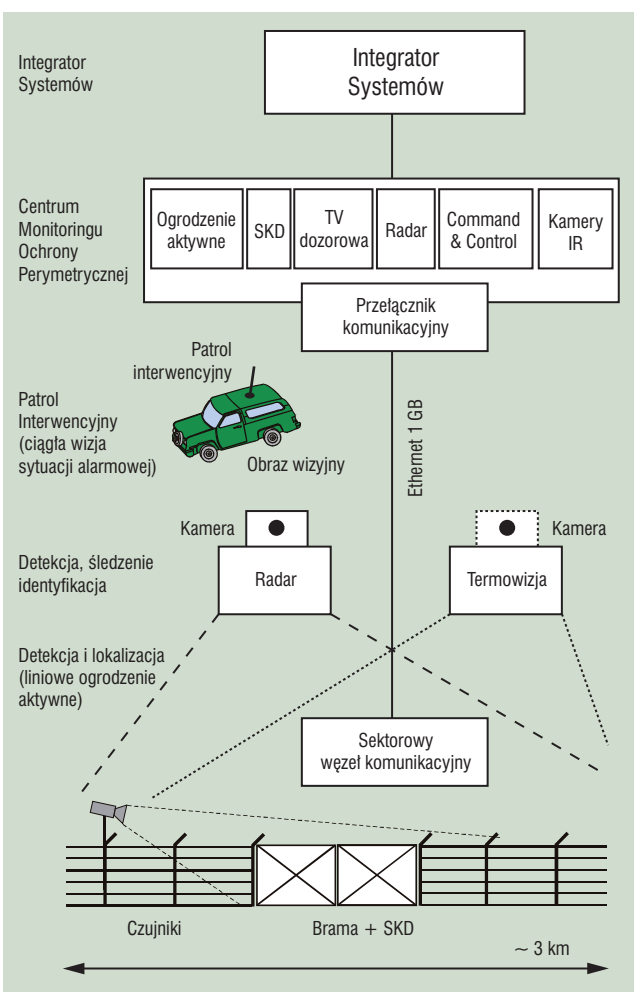
W przypadku wąskich obszarów strefy zastrzeżonej, wydłużonej wzdłuż pasa startu i lądowania, co występuje na lotniskach powojskowych, zespół kamerowy z radarem może objąć w przemiataniu dookolnym całą szerokość strefy zastrzeżonej. W sumie 2–3 zespoły radarowo-kamerowe są w stanie objąć monitoringiem 80–90% terenu lotniska. Warto w tym miejscu zaznaczyć, że stosując radarowo-kamerowy zestaw łączący aktywny radar z pasywną kamerą rejestrującą różnice termalne w polu widzenia i kamerą wizyjną, otrzymujemy zestaw „widzący” w dzień i w nocy w różnych warunkach pogodowych bez konieczności oświetlania granicy obszaru lotniska i terenu lotniska. Ponadto równolegle monitorowane są ważne obiekty portu lotniczego, np. pas startowy, droga kołowania i inne obiekty.

Wymienione zestawy radarowo-kamerowe stacjonarne lub mobilne maja podobne zastosowanie w ochronie portów morskich, granic i innych obiektów o podobnej strukturze.

3. Ewolucja sprzętowa rozpoznawania obrazowego w systemach ochrony

3.1. Kamery wizyjne

Kamery wizyjne z matrycowym czujnikiem obrazu CCD są stosowane w systemach ochrony od ponad pół wieku.



Rys. 2. Wycinek (sektor) systemu ochrony strefy zastrzeżonej portu lotniczego

Najważniejszą cechą kamery jest jakość obrazu, która zależy od wielu czynników zarówno technologicznych (doboru optyki, jakości matrycy, przetwarzania, transmisji i odtwarzania obrazu), jak i pogodowych. Ale najważniejszym kryterium pozyskania obrazu umożliwiającego rozpoznanie sceny jest poziom oświetlenia obszaru obserwacji. W praktyce oznacza to konieczność sztucznego doświetlania sceny obserwacji mimo stosowania różnych technik widzenia w warunkach słabego oświetlenia.

Ponadto matryca zobrazowania CCD stosowana w kamerach ma określoną liczbę pikseli, które są „nakładane" na pole widzenia kamery. Jeżeli pole widzenia powiększa się, to także liczba metrów kwadratowych terenu w polu widzenia jednego piksela powiększa się, a rozdzielczość obrazu maleje odwrotnie proporcjonalnie do pola widzenia. W rezultacie systemy wizyjne generalnie nie są dostosowane do obserwacji szerokokątnej, ale są bardzo użyteczne przy rozpoznawaniu sceny z odpowiednio dobranym obiektywem dostosowującym powierzchnie pola widzenia do zdolności rozdzielczej matrycy.

3.2. Kamery termowizyjne

Kamery wizyjne i termowizyjne różnią się zasadą fizyczną pozyskiwania obrazu. Kamera wizyjna rejestruje promieniowanie odbite pochodzące z postronnego (w odniesieniu do kamery i obiektu) źródła. Zasada działania kamery termowizyjnej eliminuje źródło zewnętrzne, gdyż kamera ta rejestruje kontrast termiczny miedzy obiektem i otoczeniem. Każdy obiekt w ruchu (biologiczny czy mechaniczny) generuje energię o natężeniu promieniowania termicznego (w podczerwieni) wyższą od statycznego otoczenia.

Eliminacja postronnego źródła doświetlania sceny powoduje, że dwie technologie – wizyjna i termowizyjna – wzajemnie uzupełniają się w systemach ochrony. Do niedawna głównym ograniczeniem użycia kamer termowizyjnych w systemach ochrony była cena. Wprowadzenie na rynek niechłodzonych i stosunkowo tanich termowizyjnych kamer, zbudowanych na bazie matryc bolometrycznych, udostępniło zastosowanie tej technologii w systemach ochrony.

Zasięg widzenia i kryterium detekcji rozpoznania i identyfikacji obu kamer wizyjnych i termowizyjnych są podobne i będą omówione w następnym rozdziale.

Należy jeszcze podkreślić, że mimo różnej zasady fizycznej detekcji obiektu podatność obu kamer na wpływ opadów (deszczu, śniegu) i przezroczystość atmosfery (mgły) jest zbliżona. Np. mgła lub opady powodują tłumienie fal podczerwieni 8–12 μm i 3–5 μm, na których pracują kamery termowizyjne, zatem maleje zasięg „widoczności" kamery. Ponadto opady, np. śniegu i deszczu, schładzają zarówno obiekt, jak i otoczenie niwelujące różnice temperatur – maleje więc kontrast sceny. Zatem mimo zastosowania dwóch technologii nie możemy zapewnić stałego prawdopodobieństwa wykrycia intruza na założonej odległości dla optymalnych warunków.

3.3. Radary naziemne (perymetryczne)

Radar (ang. *Radio Detection and Ranging*) jest powszechnie znany jako mikrofalowe urządzenie wykrywające obiekty latające i określające ich położenie w przestrzeni wraz ze śledzeniem ich ruchu. Zdolność przenikania mikrofal (3– 30 GHz) przez dym, mgłę, opady oraz możliwość wykrywania obiektów na ziemi (tzw. dynamiczne odtwarzanie topologii terenu) w zakresie zasięgu radaru spowodowały, że małe gabarytowo i małej mocy (rzędu dziesiątek miliwatów) naziemne radary stały się ważnym elementem w systemach ochrony.

W literaturze anglojęzycznej ten typ radarów oznacza się skrótem PSRS (*Perimeter Surveillance Radar System*) albo PSR (*Perimeter Surveillance Radar*) lub nazwą *Security Radar* i zgodnie z tym nazewnictwem znajduje on zastosowanie głównie w systemach ochrony obszarów rozległych. Rynkowo dostępne są dwa rodzaje radarów:

a) radary działające na falach centymetrowych, tradycyjnie zwanych mikrofalami, w zakresie częstotliwości 3–30 GHz, są najczęściej stosowane, mają zasięg 2–5 km przy górnej granicy częstotliwości i 5–10 km przy dolnej granicy częstotliwości;
b) radary działające na falach milimetrowych w zakresie częstotliwości 30 ÷ 300 GHz, pozwalają na uzyskanie zasięgu detekcji rzędu 1–3 km.

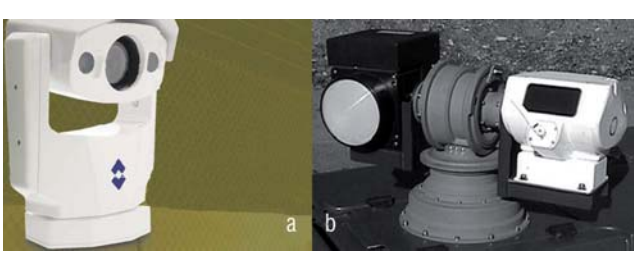
Oba typy radarów prezentują aktywną technologię w odróżnieniu od pasywnych kamer wizyjnych i termowizyjnych, zatem są mniej zależne od warunków zewnętrznych. Stosowane długości fal są również mniej tłumione przez opady i mgły niż o wiele krótsze fale widzialne lub podczerwień.

Detekcja intruza i określenie położenia (odległość, azymut) za pomocą fal elektromagnetycznych mogą być realizowane na wiele sposobów. Najprostsza jest metoda impulsowa. Powracający impuls wąskokątnej wiązki sondującej odbity od obiektu określa odległość na podstawie różnicy czasu emisji i powrotu. Kątowe położenie obracającej się anteny kierunkowej wyznacza azymut położenia obiektu.

Jeżeli radar generuje wiązkę sondującą jako fazowo koherentną (tzn. znana jest różnica fazy między impulsem generowanym a odbitym), to na podstawie efektu Dopplera możliwe jest obliczenie prędkości ruchomego obiektu, zaś efektem śledzenia obiektu jest kreślenie śladu ruchu obiektu. Zatem radar nie daje obrazu wizyjnego obiektu, lecz rzutuje na ekranie punkt symbolizujący obiekt, zaś ruch punktu po ekranie kreśli drogę fizycznego ruchu obiektu.

Cechą charakterystyczną radarów naziemnych jest możliwość szybkiego sekundowego przeszukiwania przestrzeni w zakresie 360° lub w wyznaczonym sektorze z dużym prawdopodobieństwem wykrycia w ustalonych zakresach zasięgu i małą liczbą fałszywych alarmów.

Radary naziemne zostały dostosowane przez swoje oprogramowanie do pracy w systemach zabezpieczeń jako aktywne czujniki dookolnej detekcji intruza współpracujące z czujnikami detekcji na granicy ogrodzenia. W przypadku sygnalizowania alarmu z danej strefy czujników radar zmienia tryb pracy na przeszukiwanie danej strefy.



Fot. 1. Ilustracja zestawów: a) kamerowych (kamery wizyjna i termowizyjna); b) radarowo-kamerowych (kamera po lewej stronie, radar po prawej)

Radary naziemne z reguły posiadają zdolność naprowadzania kamer termowizyjnych lub sprzężonego zestawu tych kamer na wykryty obiekt w celu ułatwienia rozpoznania i identyfikacji obiektu.

Najbardziej spektakularne jest użycie zestawu radarowo-kamerowego zbudowanego na jednej platformie obrotowej lub dwóch oddzielnych (dla radaru i zestawu kamerowego), sprzężonych z obiektywem ustawianym automatycznie na odległość podaną przez radar.

Wyposażenie radaru w odbiornik GPS umożliwia określenie pozycji radaru i naniesienie na mapie cyfrowej chronionego terenu. Dzięki temu obiekty w polu widzenia radaru są automatycznie lokalizowane na mapie chronionego terenu. Każdy nowy obiekt w terenie będzie traktowany jako generujący alarm, dopóki operator nie zaakceptuje jego pozycji. Dzięki wyposażeniu radarów w rozbudowane oprogramowanie i technikę telekomunikacyjną radary stały się kluczowymi urządzeniami w organizacji nowej generacji systemów ochrony obszarów rozległych.

4. Ewolucja oprogramowania w systemach kamerowych i radarowo-kamerowych

Analiza obrazów kamer wizyjnych, termowizyjnych i ekranów radarowych przez operatora przy dużej liczbie zestawów kamerowych lub radarowo-kamerowych jest trudna i mało efektywna. Jak wykazują badania publikowane chociażby przez Akademię Monitoringu (Kraków), operator w cyklu dwugodzinnym pracy może obsługiwać cztery monitory i do 16 kamer.

Aktualnie do analizy obrazów w systemach ochrony są aplikowane i rozwijane od ponad 20 lat technologie widzenia komputerowego (*Machine Vision*), zwane w systemach ochrony kamerami automatycznego (inteligentnego) rozpoznawania obrazów lub w skrócie kamerami inteligentnymi (*Automatic Video Surveillance* – AVS albo *Intelligent Video Surveillance* – IVS).

W kamerach lub dokładniej w systemach inteligentnych kamer odpowiednie oprogramowanie analizuje obraz wg kryteriów wprowadzanych przez operatora systemu. Zatem kamera sygnalizuje alarm w przypadku pojawienia się w polu widzenia zaprogramowanej sekwencji obrazu: człowiek, samochód, przedmiot itp.

Drugą nie mniej ważną technologią, jeszcze słabo rozpowszechnioną, jest fuzja obrazów, np. z kamery wizyjnej i termowizyjnej. Nałożenie na siebie dwóch obrazów pozyskanych w różnych technologiach poprawia wizualną jakość obrazu i skuteczność analizy komputerowej.

Najnowsze doniesienia wskazują na wprowadzenie do procesu fuzji danych pozyskanych z radaru (np. współrzędnych lokalizacji na mapie). Poniżej przybliżymy w skrócie tę problematykę.

4.1. Technologia automatycznej (inteligentnej) analizy obrazu

Technologia detekcji ruchu

Analiza ruchu (*Video Motion Detection* – VMD) była pierwszą technologią w zakresie oprogramowania mającą wspomóc operatora w analizie obrazu wizyjnego. Automatyczna detekcja ruchu była wprowadzana równolegle z cyfryzacją obrazów i cyfrowym zapisem (*Digital Video Recorder* – DVR). Oprogramowanie VMD jest do dzisiaj stosowane do analizy ruchu w polu widzenia kamer wizyjnych i termowizyjnych, jest również wykorzystywane w radarach.

Program VMD porównuje bieżący obraz pola widzenia kamery albo wydzielony obszar z poprzednim. W przypadku wykrycia zmian w porównywanych obrazach sygnalizuje alarm, a obraz z „alarmowej" kamery wyświetlany jest na ekranie operatora.

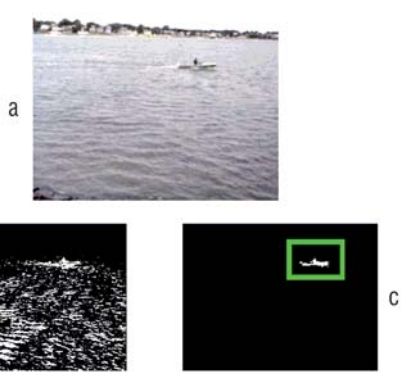
Podstawą tej technologii było założenie, że każdy ruch w obszarze sceny jest interesujący dla obserwatora. Okazało się jednak, że w przestrzeni otwartej występuje wiele poruszających się obiektów (gałęzie drzew, owady, liście itp.), które generują fałszywe alarmy. W praktyce technologia VMD znalazła zastosowanie w przypadkach pomieszczeń zamkniętych.

Inteligentna analiza obrazu (*Intelligence Video Surveillance* – IVS)

IVS jest komputerową analizą obrazu, w której program śledzi zmiany intensywności w obrębie poszczególnych pikseli. Generacja alarmu następuje wg zaprogramowanego kryterium zmiany natężenia światła grupy pikseli lub przemieszczania się zmian. Technologia aplikowana w systemach ochrony jest gałęzią głównego nurtu badań sztucznej inteligencji (*Artificial Intelligence*) w problematyce widzenia maszynowego.

Zastosowanie technologii IVS czyni kamerę (zarówno wizyjną, jak i termalną) szczególnym czujnikiem, który stosuje odpowiednie algorytmy do detekcji i śledzenia zaprogramowanego obiektu w polu widzenia kamery. IVS zawiera również algorytmy pozwalające na klasyfikacje obiektów na podstawie figury zarysowanej przez grupę „dynamicznych" pikseli i zdolna jest wyróżnić zwierzę, człowieka, samochód lub inny przedmiot. W zależności od przeznaczenia IVS może być wyposażona w algorytmy zdalnej identyfikacji osób według szczególnych cech zachowania lub cech ubioru.

IVS może być użyta do analizy obrazów kamer stacjonarnych i obrotowych po wykonaniu sekwencji obrotu. Może obsługiwać kamery czarno-białe, kolorowe, słabego oświetlenia oraz kamery termowizyjne. IVS może być stosowana wewnątrz i na zewnątrz pomieszczeń w różnych warunkach atmosferycznych. Może być również wykorzystana w różnych scenariuszach bezpieczeństwa, np. w celu detekcji intruza w systemach perymetrycznych, detekcji pozostawionych przedmiotów lub usunięcia przedmiotów obserwowanych przez kamerę, detekcji zatrzymania się lub odjazdu pojazdu



Rys. 3. Porównanie systemów analizy ruchu VMD i inteligentnej analizy obrazu IVS: a) obraz źródłowy; b) VMD – z trudem wykrywa obiekt pływający przy ruchu otoczenia; c) wyraźna detekcja obiektu

INFO-CAM
Generalny dystrybutor **AVerMedia Information, Inc.**
www.infocam.com.pl
PŁOCK Al. Kilińskiego 5, tel. (024) 266 97 12, tel./fax (024) 266 97 13, handlowy@infocam.com.pl

Różni ludzie, Różne potrzeby – Wszechstronne rozwiązania

✓ Embedded Linux

✓ D1 & 400 klatek zapis

AVerDiGi EB5416DVD PRO

- System operacyjny Embedded Linux & RTOS
- Pełna kontrola nad funkcjami za pomocą myszki
- Dwa wyjścia analogowe composite BNC, jedno wyjście VGA
- Wbudowany protokół JavaViewer umożliwiający podgląd w telefonach komórkowych
- Zdalny podgląd oraz przeglądanie nagrań za pomocą PDA
- Praca w trybie iSync umożliwia podgląd na żywo oraz odtwarzanie nagrań na tym samym ekranie jednocześnie
- Maski i pola detekcji ruchu (30x20 / 30x24 bloki)
- Prosty w konfiguracji tygodniowy kalendarz zapisu
- Tworzenie zewnętrznej kopii zapasowej z oprogramowaniem do odtwarzania
- Wbudowana wymienna kieszeń HDD SATA oraz napęd DVD+RW
- Pokrętło typu Jog shuttle ułatwiające przeglądanie archiwum
- Obsługa głowic obrotowych PTZ
- 16 wejść oraz 2 wyjścia audio

AVerMedia
www.avermedia.com
www.averdigi.eu

z obserwowanego miejsca, detekcji osoby biegnącej lub przepychającej się w grupie osób itp.

System monitoringu kamerowego wyposażony w IVS spełnia wymagania systemu zabezpieczeń w bardzo szerokim zakresie. W odniesieniu do obiektów infrastruktury krytycznej technologia IVS może być włączona w system ochrony perymetrycznej w kamerach indywidualnych lub w zestawie kamerowym (wizyjna i termowizyjna), jak również w systemach monitoringu, ruchu osobowego w terminalach, na dworcach, stadionach, w miastach itp.

Kamery wyposażone w technologię IVS mogą być włączone w dowolny system zabezpieczeń w integracji z systemem czujnikowym czy kontroli dostępu. System IVS w istotnym stopniu wyręcza w pracy operatora, ponadto podnosi skuteczność monitoringu kamerowego i generuje małą liczbę fałszywych alarmów.

4.2. Kryterium detekcji, rozpoznania i identyfikacji w systemie IVS

W systemach kamerowych przy obserwacji wizyjnej obrazu przez obserwatora są powszechnie znane zdefiniowane kryteria:

- monitorowanie tłumu, jeżeli zajmuje 5% ekranu;
- wykrycie osoby, jeżeli zajmuje 20% ekranu;
- rozpoznanie osoby, jeżeli zajmuje 50% ekranu;
- identyfikacja osoby, jeżeli zajmuje 120% ekranu.

Zdecydowanie inaczej definiuje się kryteria i pojęcia detekcji, rozpoznania i identyfikacji w systemach inteligentnej (automatycznej) analizy obrazów – IVS. W tym przypadku obowiązuje tzw. kryterium Johnsona, które zakłada, że krytyczny wymiar człowieka wynosi 0,75 m, oraz definiuje kryterium 50% prawdopodobieństwa:

- detekcji, gdy długość 0,75 m odwzorowuje 1,5 piksela, co oznacza 1,5/0,75 = 2 piksele na metr;
- rozpoznania, gdy 0,75 m odwzorowuje 6 pikseli, co oznacza 6/0,75 = 8 pikseli na metr;
- identyfikacji, gdy 0,75 m odwzorowuje 12 pikseli, co oznacza 12/0,75 = 16 pikseli na metr.

Ponadto przyjmuje się, że stojący człowiek ma wymiary 1,8 m wysokości i 0,5 m szerokości. Przeliczając powierzchnię człowieka na liczbę pikseli odwzorowania, otrzymamy: kryterium detekcji 1,8 x 2 = 3,6 piksela w pionie oraz 0,5 x 2 = 1 piksel w poziomie.

Podobnie określamy kryterium:

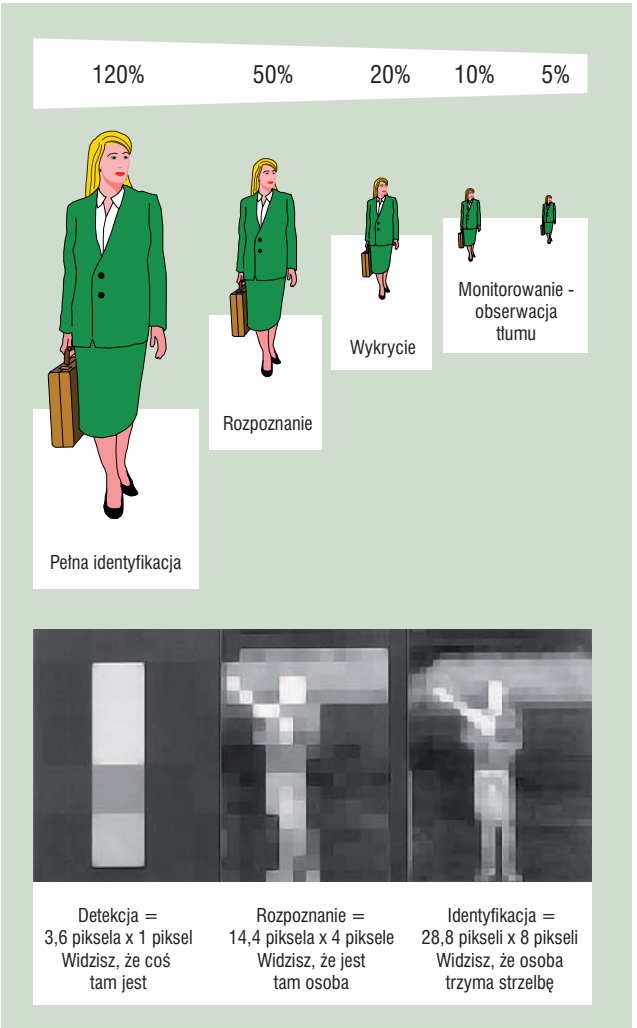
- rozpoznania: 14,4 na 4 piksele na ekranie;
- identyfikacji: 28,8 na 8 pikseli na ekranie.

Graficzne przedstawienie powyższych wyliczeń obrazuje rys. 4, na którym dla kontrastu zestawiono kryteria telewizji obserwacyjnej i telewizji widzenia komputerowego.

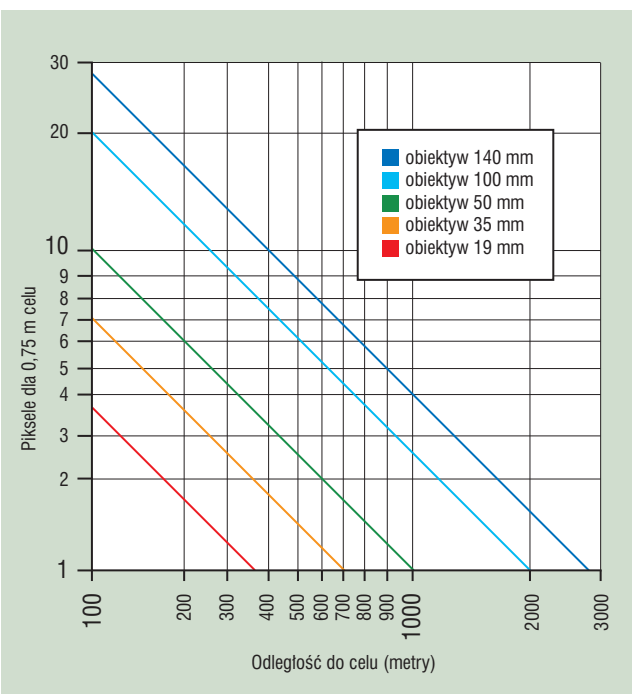
W przypadku automatycznej analizy obrazu kryteria rozpoznania określa się jako:

- detekcję – oznacza to wykrycie obecności obiektu w polu widzenia (jest lub nie ma);
- rozpoznanie – oznacza to określenie rodzaju obiektu w sensie zwierzę, człowiek, samochód;
- identyfikacja – ma tutaj wojskowe znaczenie: swój czy obcy, w praktyce cywilnej oznacza możliwość określenia np. posiadania przedmiotów, bagażu itp.

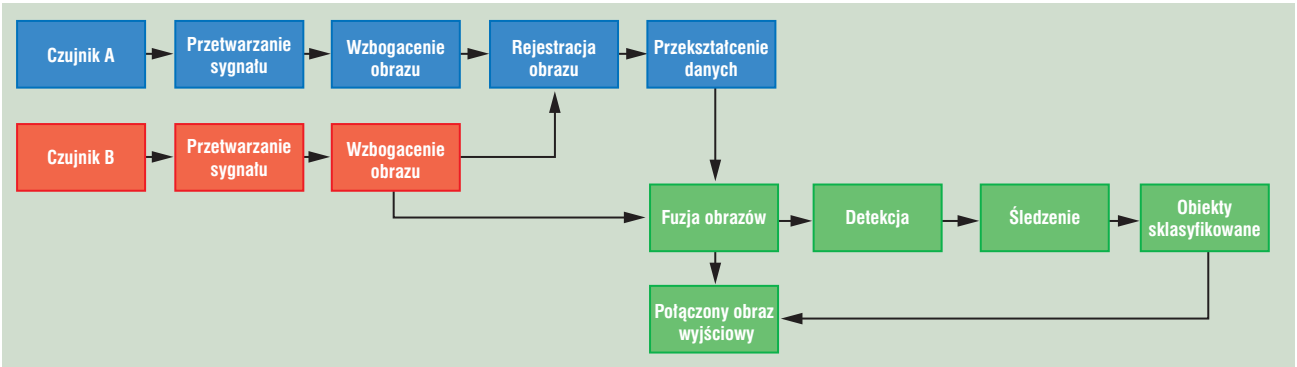
Oczywiste jest, że obraz człowieka odwzorowany na matrycy zobrazowania kamery zależy od pola obserwacji, które z kolei jest funkcją parametrów obiektywu i odległości.



Rys. 4. Kryteria detekcji, rozpoznania i identyfikacji w analizie obrazu przez człowieka (góra) i przy automatycznej analizie komputerowej (dół) – analiza automatyczna na przykładzie kamery termowizyjnej wg prospektu firmy FLIR



Rys. 5. Nomogram bolometrycznej kamery termowizyjnej z matrycą 320 x 280 pikseli (wymiar piksela 38 µm)



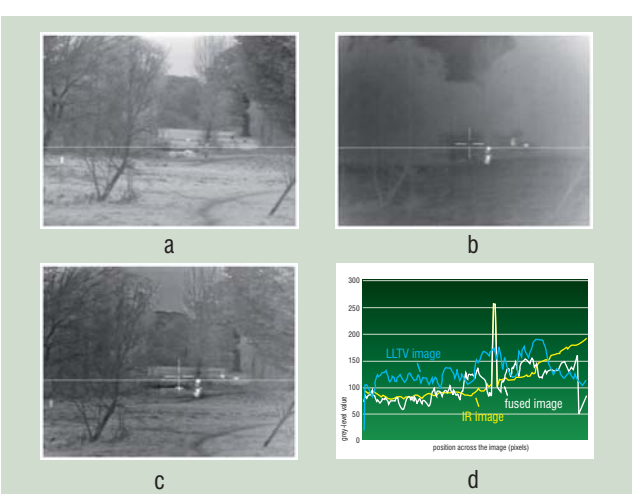
Rys. 6. Schemat procesu fuzji (nakładania) obrazów pozyskanych z kamer różnych technologii

Zdolność automatycznego rozpoznawania obrazu w funkcji odległości podaje się w formie znormalizowanych nomogramów (jak na rys. 6) dla matryc o określonej liczbie pikseli i wymiarach piksela. Z liczby pikseli na 0,75 metra dla danej odległości oblicza się liczbę pikseli na metr i na człowieka, skąd wynika zdolność detekcji, rozpoznania, identyfikacji w funkcji odległości (jak na rys. 5).

W praktyce jednak należy uwzględnić warunki atmosferyczne (tłumienie), uwarunkowania kontrastu obrazu i tła. Dla kamer wizyjnych oznacza to oświetlenie i współczynnik odbicia światła obrazu i tła, a dla kamer termowizyjnych to różnica temperatury obrazu i tła. Zatem analizę parametrów konkretnej kamery, podawanych zwykle dla warunków optymalnych, należy odnieść do spodziewanych parametrów w warunkach ekstremalnych.

4.3. Fuzja obrazów

Jednoczesne pozyskanie obrazu z kamer różnej technologii, np. wizyjnej i termowizyjnej, zapewnia optymalne widzenie (na miarę dysponowanej techniki) w dzień/noc i w różnych warunkach pogodowych. Ale w rozdzielnej technologii przetwarzania obrazu otrzymujemy obrazy na różnych monitorach z wadami właściwymi każdej technologii, np. w przypadku kamer wizyjnych: słabo kontrastowe obrazy w nocy i przy złej pogodzie, na dużych odległościach w przypadku kamer termowizyjnych: mała rozdzielczość (brak szczegółów), słaby kontrast przy opadach, trudna intuicyjna interpretacja obrazu na dużych odległościach.



Rys. 7. Fotograficzna prezentacja wyników fuzji obrazów z dwóch kamer: a) obraz kamery wizyjnej, b) obraz kamery LWiR, c) obraz wynikowy fuzji, d) sygnatury pojedynczych obrazów i złożonego obrazu

Technologia fuzji, czyli nałożenie obu obrazów z kamer różnych technologii i prezentacja wynikowego obrazu na jednym ekranie, poprawia jakość obrazu, niwelując słabsze strony łączonych technologii, oraz zwiększa efektywność i komfort pracy operatora [6.7].

Na rys. 6 przedstawiamy schemat fuzji obrazów jako procesu wstępnego przed poddaniem inteligentnej analizie (IVS) już wspólnego obrazu.

Na rys. 7 pokazano fotografie prezentujące obrazy pojedynczych kamer i efekt fuzji. Najbardziej wyrazisty jest efekt sygnatury na rysunku 7d, otrzymany w wyniku analizy linii poziomej przecinającej obraz. Analiza linii pokazuje, że największy kontrast obiektu względem otoczenia daje obraz otrzymany w wyniku fuzji. Zatem obraz łączny poddany procesowi komputerowej analizy IVS istotnie zwiększa prawdopodobieństwo właściwego rozpoznania obrazu. Zwiększenie prawdopodobieństwa detekcji obiektu do poziomu 99% daje wprowadzenie do procesu fuzji obrazów z kamer danych radarowych. System wizyjny odwzorowuje kształt obiektu na ekranie, podczas gdy radar podaje odległość, azymut (lokalizuje na mapie) oraz kierunek ruchu i prędkość. Posiadając kształt obiektu i odległość, można określić przekrój obiektu (w pionie i poziomie) w celu jego klasyfikacji. Wykrywany obiekt jest prowadzony radarem z takim sterowaniem pola widzenia kamer, aby utrzymać obiekt w środku pola widzenia, co umożliwia ciągłą weryfikację identyfikacji obiektu. W całym procesie śledzenia ruchu obiektu algorytm automatycznego rozpoznania dokonuje ciągłej korelacji wymiarów obiektu, odległości i szybkości.

Fuzja danych trzech sensorów – kamer wizyjnych i termowizyjnej oraz radaru – daje najbardziej wiarygodne i skuteczne wyniki automatycznej detekcji, rozpoznania i identyfikacji obiektu w systemach ochrony.

5. Ewolucja teletransmisji w systemach ochrony

Wiele systemów ochrony oferowanych zwłaszcza przez duże firmy bazuje na własnych wewnątrzsystemowych protokołach transmisji i dedykowanych sterownikach. Systemy takie nazywamy zamkniętymi z uwagi na trudności z dołączeniem urządzeń innych firm. Ale zagrożenia terrorystyczne, zwłaszcza w odniesieniu do obiektów infrastruktury krytycznej, wymagają integracji nie tylko samych technicznych systemów ochrony, takich jak SSWiN, SKD, telewizja dozorowa, systemy perymetryczne, ochrona fizyczna, ale i zapewnienia wymiany informacji, w tym obrazowej, ze sztabem zarządzania bezpieczeństwem i służbami odpowiedzialnymi

za bezpieczeństwo. Ponadto obserwujemy istotny wzrost informatyzacji systemów ochrony. Między innymi stąd wynika dążenie do budowy technicznych systemów ochrony na bazie profesjonalnych teleinformatycznych systemów spełniających wymagania telekomunikacji wewnątrzsystemowej, coraz bardziej zinformatyzowanych systemów i wymagania otwartej telekomunikacji w ramach organizacji zarządzania bezpieczeństwem.

Protokół internetowy (IP) implementowany w sieci Ethernet (głównie światłowodowej) i sieciowe elementy systemu (zwłaszcza urządzenia inteligentnej analizy obrazu) tworzą obecnie sieciocentryczne inteligentne systemy teletransmisyjne, które są bazą nowej generacji zintegrowanych systemów ochrony.

5.1. Ewolucja analogowej CCTV do sieciowej telewizji z automatyczną analizą obrazów

Najbardziej spektakularny przykład ewolucji technologii teletransmisji w systemach ochrony można przedstawić na przykładzie ewolucji transmisji od telewizji analogowej do cyfrowych inteligentnych systemów wizyjnych.

Typowy system telewizji analogowej to kamera połączona z monitorem kablem koncentrycznym przez krosownicę (multiplekser z zapisem kasetowym). System wewnętrznie zamknięty był odwzorowany w nazwie *Closed Circuit Television* – CCTV.

Ewolucję systemów bezpieczeństwa, w tym telewizji dozorowej, stymuluje stopniowe przenikanie technologii informatycznych do przemysłu *security*. Istotny wpływ na informatyzację systemów ochrony wywarły:

- cyfryzacja i cyfrowe przetwarzanie obrazu (umożliwiły kompresję obrazu, cyfrową transmisję i cyfrowe odtwarzanie),
- adaptacja technologii widzenia komputerowego (umożliwiła automatyzację analizy i fuzji obrazów),
- adaptacja sieci teleinformatycznych z oprzyrządowaniem i oprogramowaniem sieciowym (stworzyła otwartą sieć integrującą systemy ochrony).

Informatyzacja przeniknęła nie tylko do systemów, ale i do poszczególnych urządzeń.

Na rys. 9 przedstawiono inteligentną kamerę sieciową firmy AXIS, wykorzystującą technologię przetwarzania obrazu. Wprowadzenie inteligentnych kamer, czujników i innych czujek rewolucjonizuje konfiguracje systemów ochrony, co ewidentnie widać na rys. 10 przedstawiającym schemat inteligentnej telewizji sieciowej.

W sieciowej inteligentnej telewizji wszystkie nowe technologie, takie jak cyfryzacja, kompresja, zapis, IVS, interfejs sieciowy, mogą być zastosowane bezpośrednio w kamerach.

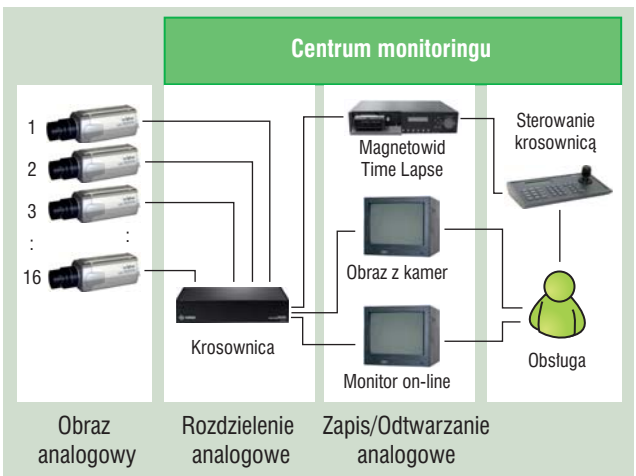
5.2. Sieciowa integracja systemów ochrony

Sieciowy, teleinformatyczny system telekomunikacji wewnątrzsystemowej jest budowany na strukturze sieci *Ethernet* z elementami oprzyrządowania *First Ethernet* – 100Mb/s i *Gigabit Ethernet* – 1 Gb/s. Mniejsze sieci mogą występować w konfiguracji 10/100 Mb/s *Ethernet*.

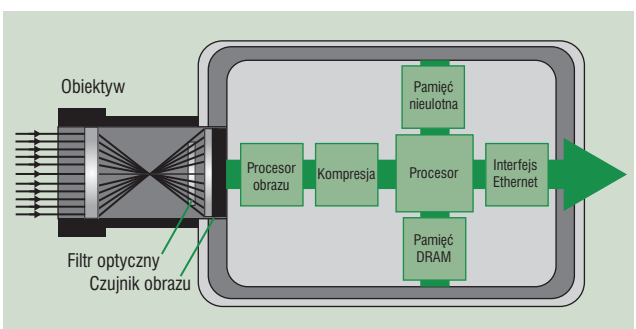
Na rys. 11 przedstawiono szkielet modelowej struktury sieciowej proponowanej dla systemu ochrony.

Strukturę sieci tworzą profesjonalne urządzenia typowej sieci teleinformatycznej, takie jak przełączniki i rutery, umożliwiające zarządzanie siecią. Serwer kamer i media-konwertery występują tutaj jako interfejsy sieciowe do podłączenia urządzeń ochrony: kamer analogowych, czujek, czytników.

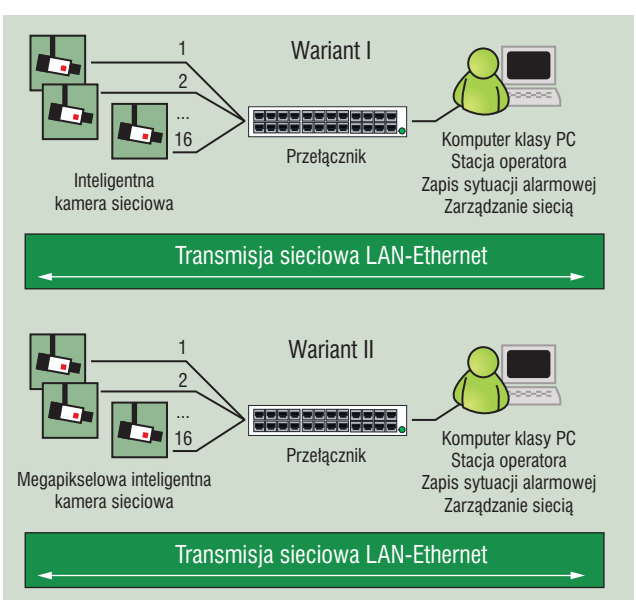
Urządzenia końcowe w postaci serwerów, stacji roboczych są wyposażone w standardowe interfejsy sieciowe. Przedstawiona na rys. 11 struktura sieci z oprogramowaniem sieciowym, uzupełniona o oprogramowanie aplikacyjne, sieciowe serwery, inteligentną analizę obrazu oraz sieciowe urządzenia rejestracji obrazów, staje się szkieletową strukturą integrującą system ochrony, czyli *Intelligence Network Security System*.



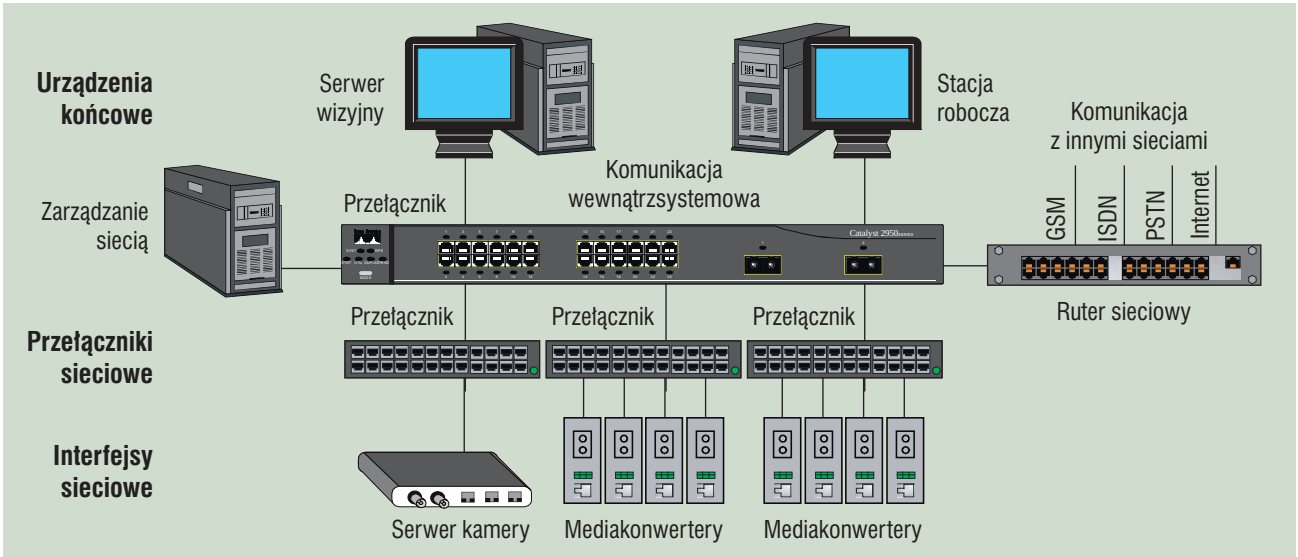
Rys. 8. Analogowy system CCTV z zastosowaniem multipleksera



Rys. 9. Przykładowa inteligentna kamera sieciowa firmy AXIS



Rys. 10. W pełni sieciowy system wideo z inteligentnymi kamerami sieciowymi



Rys. 11. Schemat szkieletowej sieci teleinformatycznej do zastosowań w systemach ochrony

6. Zakończenie

W pracy przeanalizowano trendy rozwojowe optoelektronicznych i radarowych urządzeń detekcji i zobrazowania w odniesieniu do systemów ochrony obiektów infrastruktury krytycznej.

Organizacja i struktura systemów ochrony jest uzależniona od technicznych i informatycznych możliwości stosowanych urządzeń. W ochronie dużych obiektów, jakimi są obiekty infrastruktury krytycznej, niezbędne staje się stosowanie:

- mieszanych technologii detekcji (np. ogrodzeniowych czujników i radarów naziemnych),
- mieszanych technologii zobrazowania w warunkach dzień/noc (np. kamer wizyjnych i termowizyjnych),
- mieszanych technologii naprowadzania i śledzenia (np. radaru i zestawu kamer wideo oraz dodatkowo kamery termowizyjnej),
- technologii automatycznego rozpoznawania, identyfikacji w czasie śledzenia intruza, w tym inteligentnego rozpoznania i fuzji obrazów z kilku czujników.

Skuteczne przeciwdziałanie integruje systemy, ludzi i procedury działania. Wymaga więc inteligentnej struktury integracyjnej. Aktualnym rozwiązaniem staje się sieciocentryczna struktura teleinformatyczna w konfiguracji sieci IP Ethernet. Szkielet sieci buduje się na profesjonalnych urządzeniach sieci teleinformatycznych, takich jak komputery, przełączniki, rutery – z konwerterami służącymi jako interfejsy do podłączenia urządzeń ochrony.

Sieciowy, teleinformatyczny system komunikacji wewnątrzsystemowej oraz automatyczna analiza obrazów stymuluje przemysł urządzeń *security*, zwłaszcza optoelektronicznych kamer do produkcji inteligentnych urządzeń sieciowych. Zatem rozwój technologii informatycznych i ich przenikanie do systemów ochrony rewolucjonizuje struktury systemów ochrony, a zwłaszcza obiektów infrastruktury krytycznej.

Mieczysław Szustakowski
Wiesław Ciurapiński
Janusz Wróbel
Instytut Optoelektroniki
Wojskowa Akademia Techniczna

Literatura

1. GAO – 04-728 Aviation Security: *Further Steps Needed to Strengthen the Security of Commercial Airport Perimeter and Access Control*. www.gao.gov./new.items/do4728.pdf
2. Airport Security Transportation – THALES.
3. F. Kapounek, M. Maki Inteli Fiber – *The Next Generation Optic Fence Sensor* 35th Annual 2001 ICC on Security Technology, London.
4. M. Szustakowski, W. Ciurapinski, N. Palka, M. Zyczkowski: *Recent Development of Fibre Optic Sensors for Perimeter Security*, 35th Annual 2001 ICC on Security Technology, London.
5. T. Riley, M. Smith: *Image Fusion Technology for Security and Surveillance Application*. Proc. of SPIE, Vol. 6402.
6. M. Smith, J.P. Heather: *Review of Image Fusion Technology in 2005*, Proc. of SPIE, Vol. 5782.
7. A. J. Lipton, Craig H. Heartwell: *Critical Asset Protection, Perimeter and Threat Detection Using Automated Video Surveillance*. www.objectvideo.com.
8. K. Sage, S. Young, 32nd Annual 1998 ICC on Security Technology.
9. A. J. Lipton, H. Fujiyoshi, R. S. Patil: *Moving Target Detection and Classification from Real-Time Video*, Procc. of the IEEE Workshop on Application of Computer Vision. 1998.
10. C. J. Baker, H. D Griffits: *Bistatic and Multistatic Radar Sensor for Homeland Security*, www.nato-asi.org/sensors2005/papers/baker.pdf.
11. P. Cory, H. R. Everett, Tracy Heath Pastore: *Radar – Based Intruder Detector for a Robotic Security System*, www.nosc.mil/robots/pubs/spie3525b.pdf.
12. A. Browne, M. Bissonnett: *High Resolution Millimeter Wave (MMW) Perimeter Surveillance Radar*, www.amphitech.com/pdf/PSRwpMay2006.pdf.
13. Technical guide to network video, www.axis.com.
14. Mark Morris: *Teleinformatics*, J. Willey ltd., 2000.
15. FFT Secure Fence installation overview, www.fft.com.au.
16. B. Hennessey, R. B. Wesson: *Security Simulation for Vulnerability Assessment*, Proceedings of the SPIE, Volume 6227, pp. 622708 (2006).

SERIA CZUJEK CYFROWYCH DSC

Precyzyjna cyfrowa technologia opracowana przez firmę DSC pozwala wykryć intruza, redukując tym samym ilość fałszywych alarmów do minimum.

Na terenie prywatnych posiadłości, jak i w budynkach biurowych, seria czujek LC usprawnia system alarmowy, zapewniając niezawodność działania również podczas najbardziej wymyślnych prób włamania.

Dodatkowo smukła linia obudowy, odporność na zwierzęta, prosta instalacja, różne sposoby montażu, odporność na światło białe oraz wiele innych właściwości powoduje, że nowa seria czujek jest niezwykle atrakcyjnym produktem.

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

LC-100-PI Czujka PIR odporna na zwierzęta

Wymiary ..... 92mm x 62,5mm x 40mm
Waga 61g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie ..... od 8,2 do 16V=
Pobór prądu (czuwanie) ..... 8 mA (± 5%)
Pobór prądu (działanie) ..... 10 mA (± 5%)
Sabotaż: styk NC ..... 0,1A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10V/m 80-1000 MHz
• statyczne ..... 8kV kontakt, 15kV powietrze
• przepięciowe..... 2,4kV@1,2J

LC-101-CAM Czujka PIR z kamerą (czarno-biała/kolorowa),odporna na zwierzęta

Wymiary ..... 116mm x 62,5mm x 40mm
Waga 112g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie ..... od 8,2 do 16V=
Pobór prądu (czarno-biała) ..... 115 mA
Pobór prądu (kolorowa) ..... 150 mA
Sabotaż: styk NC ..... 0,1A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10V/m 80-1000 MHz
• statyczne ..... 8kV kontakt, 15kV powietrze
• przepięciowe..... 2,4kV@1,2J

LC-102-PIGBSS Czujka PIR oraz zbicia szyby, odporna na zwierzęta

Wymiary ..... 118mm x 62,5mm x 41mm
Waga 83g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie ..... od 8,2 do 16V=
Pobór prądu (czuwanie) ..... 16,5 mA
Pobór prądu (działanie) ..... 22 mA
Sabotaż: Styk NC ..... 0,1A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10V/m 80-1000 MHz
• statyczne ..... 8kV kontakt, 15kV powietrze
• przepięciowe..... 2,4kV@1,2J

LC-103-PIMSK Czujka PIR + mikrofala z antymaskingiem, odporna na zwierzęta

Wymiary ..... 118mm x 62,5mm x 41mm
Waga 102g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR) + mikrofala Doppler
Zasilanie ..... od 8,2 do 16V=
Pobór prądu (czuwanie) ..... 18 mA
Pobór prądu (działanie) ..... 25,5 mA
Sabotaż: styk NC ..... 0,1A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10V/m 80-1000 MHz
• statyczne ..... 8kV kontakt, 15kV powietrze
• przepięciowe..... 2,4kV@1,2J

LC-104-PIMW Czujka PIR + mikrofala

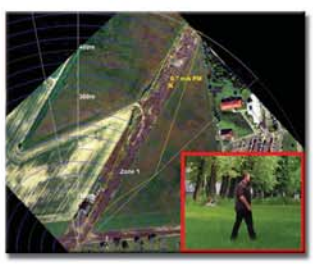
Wymiary ..... 118mm x 62,5mm x 41mm
Waga 102g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR) + mikrofala Doppler
Zasilanie ..... od 8,2 do 16V=
Pobór prądu (czuwanie) ..... 18 mA
Pobór prądu (działanie) ..... 25,5 mA
Sabotaż: styk NC ..... 0,1A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10V/m 80-1000 MHz
• statyczne ..... 8kV kontakt, 15kV powietrze
• przepięciowe..... 2,4kV@1,2J

LC-105-DGB Czujka zbicia szyby

Wymiary ..... 79mm x 48mm x 21mm
Waga 40g
Zasięg ..... 10m max
Zasilanie ..... od 9 do 16V=
Pobór prądu (czuwanie) ..... 15 mA @ 12 V=
Pobór prądu (działanie) ..... 40 mA @ 24 V=
Sabotaż: styk NC ..... 50mA @ 24 V=
Odporność na zakłócenia:
• radiowe ..... 10V/m 80-1000 MHz
• statyczne ..... 8kV kontakt, 15kV powietrze
• przepięciowe..... 2,4kV@1,2J

KABE

WYZNACZAMY NOWE GRANICE OCHRONY



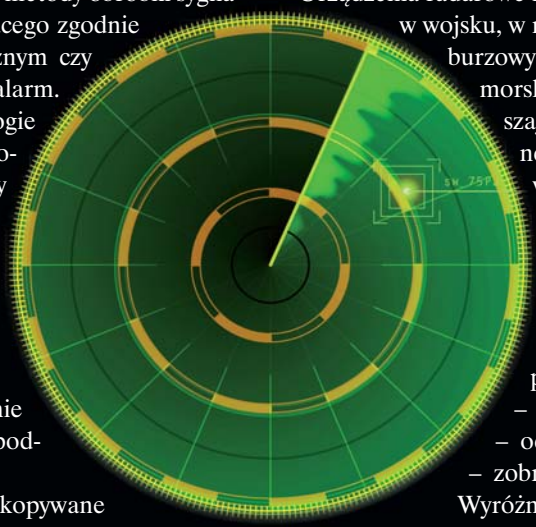
Nasze systemy radarowe wykrywają każde wtargnięcie osób i pojazdów na chroniony obszar, stale monitorując aktualną pozycję intruza. Radary automatycznie sterują zespołem kamer tworząc w pełni zintegrowany system ochrony.

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

WYKORZYSTANIE RADARÓW W OCHRONIE ZEWNĘTRZNEJ OBIEKTÓW

Wstęp

Systemy ochrony rozległych obiektów strategicznych lub infrastruktury krytycznej, do których (w terminologii europejskiej) zalicza się bazy wojskowe, lotniska, magazyny sprzętu wojskowego i paliw, zbiorniki wodne itp., są rozwijane i stosowane od niemal ćwierć wieku. Dlatego kryteria podziału czujników do ochrony zewnętrznej obiektów są łatwo identyfikowalne. Urządzenia można wyróżnić według sposobu i miejsca instalacji, stosowanej w nich metody obróbki sygnału, rodzaju użytego czujnika działającego zgodnie ze ściśle określonym prawem fizycznym czy też według czynnika powodującego alarm. Wykorzystują one głównie technologie czujników liniowych o zasięgu strefowym (200–300 m), przyjmujące nazwy od sposobu rozmieszczania czujników:



– czujniki ogrodzeniowe, punktowe i kablowe (elektryczne i światłowodowe) rozmieszczane na ogrodzeniu,
– czujniki naziemne – to głównie aktywne bariery mikrofalowe i podczerwieni oraz radary,
– czujniki ziemne – kablowe zakopywane w gruncie na głębokości rzędu 15–30 cm, elektryczne, magnetyczne, światłowodowe, ciśnieniowe itp.

Niniejszy artykuł jest poświęcony technice radarowej i jej wykorzystaniu w ochronie zewnętrznej obiektów.

Podstawowe informacje o technice radarowej

Radar jest to urządzenie służące do wykrywania za pomocą fal radiowych obiektów powietrznych, nawodnych oraz lądowych, takich jak samoloty, śmigłowce, rakiety, statki (również chmury oraz obiekty terenowe), pozwalające na określenie kierunku, odległości, a także wielkości obiektu, a w przypadku radarów dopplerowskich służące także do pomiarów prędkości wykrywanego obiektu.

„Radar" to słowo utworzone na początku lat czterdziestych XX w. z pierwszych liter angielskiego terminu *Radio Detection And Ranging* (oznaczającego wykrywanie oraz wyznaczanie odległości za pomocą fal radiowych). Wcześniejszy termin brytyjski RDF (*Radio Direction Finding*) został zastąpiony jego amerykańskim odpowiednikiem, który przyjął się w wielu językach.

W radarach wykorzystuje się do wykrywania obiektów zjawisko odbicia fal radiowych od wykrywanych obiektów (najczęściej w tym celu wykorzystuje się pasmo mikrofal, a więc od 1 GHz do 300 GHz) lub fale wysyłane przez te obiekty.

W radarze aktywnym nadajnik radaru emituje wiązkę promieniowania oświetlającą badany obszar, sygnał odbija się od obiektu i jest odbierany w odbiorniku znajdującym się zazwyczaj w tym samym miejscu co nadajnik.

Radar pasywny nie emituje promieniowania, a jedynie odbiera promieniowanie wysyłane najczęściej w celach komunikacyjnych przez samoloty, a w astronomii przez obiekty kosmiczne. Docierający do odbiornika sygnał jest bardzo słaby, dlatego trzeba konstruować odpowiednie anteny i odbiorniki umożliwiające określenie kierunku, natężenia fali i jej inne parametry.

Urządzenia radarowe mają obecnie wiele zastosowań, np. w wojsku, w meteorologii do wykrywania chmur burzowych, w kontroli ruchu lotniczego, morskiego, w kontroli prędkości poruszających się pojazdów przeprowadzanej przez policję. Tabela 1 przedstawia podstawowy podział urządzeń radarowych wraz z określeniem wykorzystywanego przez nie zakresu częstotliwości fal elektromagnetycznych.

Praca radaru obejmuje trzy etapy (rys. 1):
– nadawanie,
– odbiór,
– zobrazowanie.

Wyróżniamy dwa typy radarów:
– **impulsowy**, wykorzystujący do pomiaru odległości pomiędzy urządzeniem a celem pomiar czasu sygnału przebywającego drogę nadajnik – cel – odbiornik,
– **dopplerowski**, wykorzystujący pomiar zmiany częstotliwości fali odbitej od celu zgodnie z efektem Dopplera.

Radar impulsowy

Radar impulsowy umożliwia ocenę odległości między radarem a celem poprzez pomiar czasu przejścia sygnału z anteny do celu i z powrotem. Rys. 2 przedstawia zasadę pomiaru w przypadku tego typu radaru.

Dzięki zastosowaniu w radarze impulsowym bardzo stabilnych generatorów częstotliwości oraz układów mierzących czas pomiędzy momentami nadania i odbioru sygnału z dużą dokładnością można wskazać położenie obiektu, a także odróżnić od siebie obiekty znajdujące się w tym samym kierunku od anteny, ale w różnych odległościach.

W wielu przypadkach nadajnik oraz odbiornik radaru posiadają wspólną antenę oraz układ przełącznika nadawanie – odbiór, który separuje obydwa układy, zapobiega przedostaniu się sygnału o dużej mocy z nadajnika do czułego układu odbiornika, a także odpowiednio ukierunkowuje w trakcie falowodowym drogę sygnału.

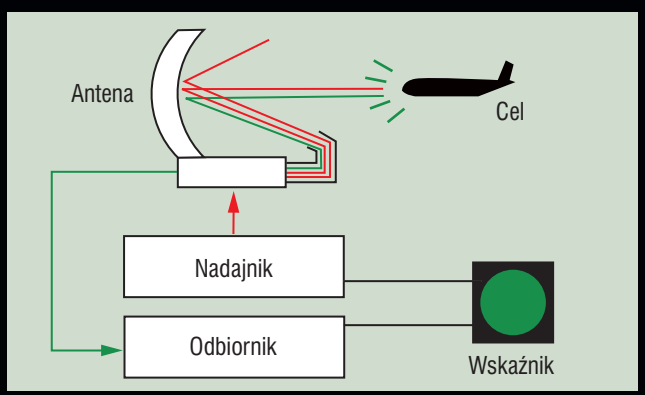
Urządzenie posiadające jedną antenę nadawczo-odbiorczą musi bazować na pewnych kompromisach konstrukcyjnych, które są wymuszone przez zjawiska fizyczne. By zapewnić widzialność obiektów znajdujących się w niewielkiej odległości, należy skrócić czas trwania sygnału sondującego,

[GHz]											
0,1	0,3	0,5	1	2	4	8	12	18		60	100
VHF	UHF		L	S	C	X	K_u	K	K_a	E, W	
			MIKROFALE								
Radary naziemne i okrętowe dalekiego zasięgu: wczesne ostrzeganie, kontrola obszaru powietrznego, telemetria (IFF), radionawigacja (MLS)											
			Radary naziemne, okrętowe i lotnicze średniego zasięgu: kontrola obszaru powietrznego, naprowadzanie lotnictwa myśliwskiego, obserwacja powierzchni ziemi								
						Radary naziemne, okrętowe i lotnicze bliskiego zasięgu: obserwacja powierzchni ziemi, śledzenie celów i kierowanie uzbrojeniem, obserwacja obszarów chronionych					

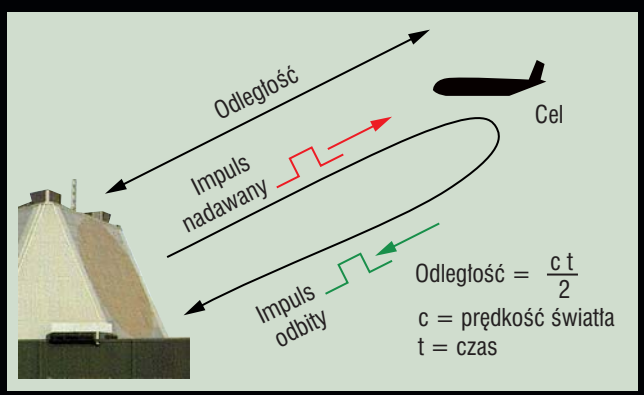
Tab. 1. Zakresy częstotliwości stosowane w technice radarowej

tak aby echo od pobliskiego obiektu nie dotarło do anteny jeszcze w czasie nadawania sygnału. Jednocześnie czas trwania impulsu przekłada się bezpośrednio na zasięg radaru, więc nie jest możliwe dowolne skrócenie czasu trwania impulsu, ponieważ w ten sposób traci się na jego podstawowej zalecie, czyli zasięgu. Odbite od celu echo nie powinno również wracać do urządzenia w momencie nadawania kolejnego impulsu. Konieczny jest więc taki dobór czasu powtarzania, czyli odstępu czasowego pomiędzy kolejnymi emitowanymi impulsami, aby do takiego zjawiska nie doszło. W związku z tym, w zależności od przeznaczenia urządzenia, wyróżnia się radary o krótkim czasie trwania impulsu i krótkim czasie powtarzania – radary do pomiaru odległości celów w najbliższym otoczeniu (np. radary pola walki, radary portowe) – oraz urządzenia z impulsami o długim czasie trwania i długim czasie powtarzania – radary o dużym zasięgu (np. radary wczesnego ostrzegania).

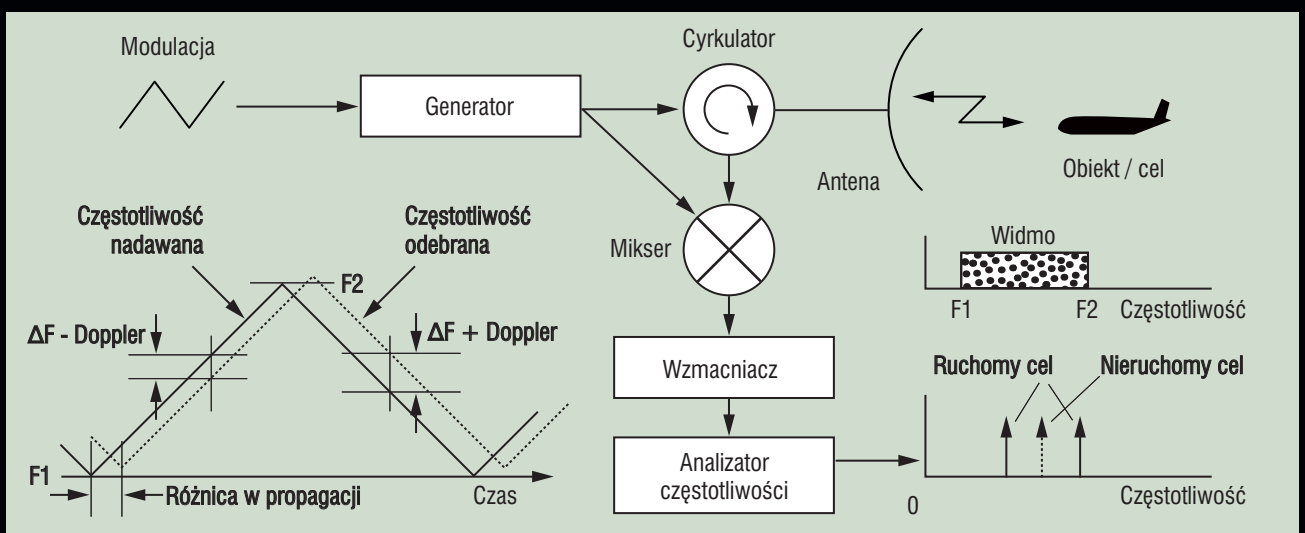
Podstawowym parametrem technicznym stosowanym w celu porównania radarów impulsowych jest częstotliwość powtarzania sygnału, czyli odwrotność czasu powtarzania, opisująca liczbę emitowanych impulsów przez nadajnik radaru w ciągu sekundy. Jest to jeden z bardziej istotnych parametrów w urządzeniach z mechanicznie sterowaną anteną. Ustawiając odpowiednią częstotliwość powtarzania, można zapewnić dość gęste pokrycie przestrzeni sygnałem sondującym, dzięki czemu maleje ryzyko, że któryś z celów nie zostanie opromieniony przez wiązkę radarową.



Rys. 1. Zasada działania radaru



Rys. 2. Pomiar odległości za pomocą radaru impulsowego



Rys. 3. Zasada działania radaru dopplerowskiego

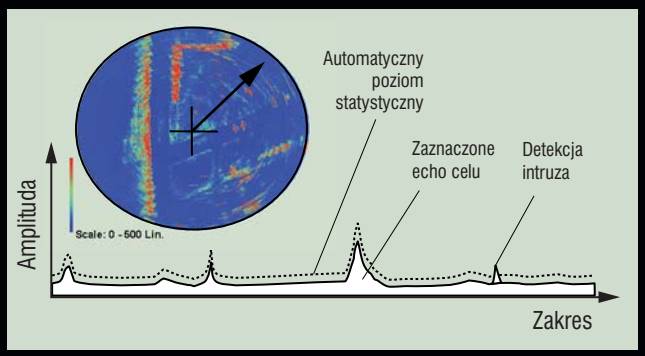
Radar dopplerowski

W radarze dopplerowskim wykorzystywane jest zjawisko przesunięcia dopplerowskiego wywołanego ruchem obiektów, na których następuje odbicie. Radar dopplerowski jest przykładem aktywnej teledetekcji w mikrofalach.

Wyróżnia się trzy typy radarów dopplerowskich:
- impulsowe – wysyłają krótkie impulsy o dokładnie określonej częstotliwości i czasie trwania impulsu,
- o wiązce ciągłej – cały czas wysyłają wiązkę promieniowania o określonej częstotliwości,
- o wiązce modulowanej częstotliwościowo (FM).

Przy odbiorze wiązki w radarach, w zależności od typu radaru, analizuje się natężenie odbieranej wiązki, czas powrotu wiązki, a w radarach dopplerowskich dodatkowo jej częstotliwość, na podstawie której określa się prędkość poruszającego się obiektu.

Radar dopplerowski jest stosowany nie tylko do wykrywania obiektów i określania ich położenia, ale także do określania kierunku (zbliżanie – oddalanie) i prędkości poruszania się.



Rys. 4. Typowa odpowiedź FFT radaru dla jednego kąta

Radary perymetryczne

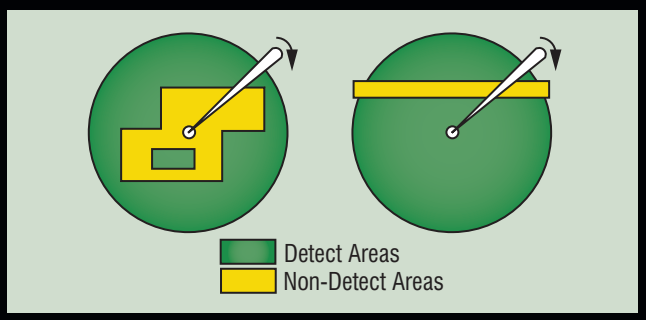
Nowoczesny system zabezpieczenia perymetrycznego powinien nie tylko wykrywać fakt naruszenia strefy chronionej, lecz również wskazać miejsce tego naruszenia oraz położenie i kierunek przemieszczania się intruza. Daje to możliwość szybkiej i skutecznej reakcji na powstałe zagrożenie. Dokładna lokalizacja intruza znacznie podnosi również bezpieczeństwo jednostki reagującej.

Skuteczna ochrona perymetryczna powinna zawierać czujniki obserwujące teren poza ogrodzeniem w celu wykrycia nie tylko rzeczywistych, ale i potencjalnych intruzów. Jest to bardziej uciążliwe dla ochrony obiektu, ale jednostki ochrony fizycznej mogą wówczas znacznie wcześniej podjąć przygotowanie do interwencji, jeżeli nastąpi rzeczywiste naruszenie strefy chronionej.

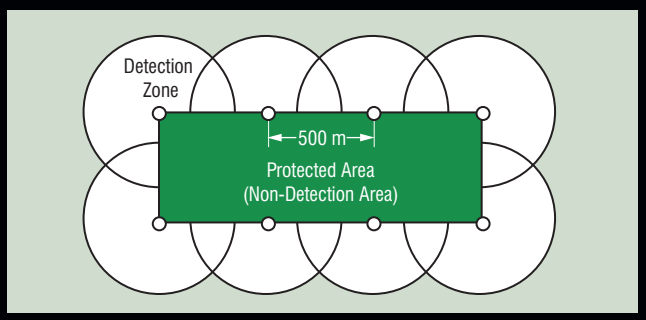
Radar perymetryczny (*Perimeter Surveillance Radar* – PSR) jest radarem przeznaczonym do monitorowania aktywności wokół obiektów (najczęściej specjalnych), takich jak porty lotnicze, porty morskie, obiekty wojskowe, granice państw, rafinerie i inne. Może wykorzystywać **dopplerowską metodę detekcji** – wymagany jest wtedy ruch intruza w kierunku radaru – albo **mapowanie** (ang. *clutter mapping*) – ruch może odbywać się wtedy w dowolnym kierunku.

Radary perymetryczne przeznaczone są do wykrywania ruchu obiektów naziemnych, takich jak idący lub czołgający się ludzie albo pojazdy (rys. 5). Technologie radarowe z natury przystosowane są do monitorowania dużych obszarów, dlatego możliwy jest **zakres ich pracy od kilkuset metrów**

Rys. 5. Idea zastosowania radarów perymetrycznych



Rys. 6. Maska obszarów [1]



Rys. 7. Ochrona przy pomocy radarów perymetrycznych [1]

do 10 km. Umożliwiają one śledzenie pełnego koła (360°) lub jego wycinka (80–180°), stale analizując sygnały zwrotne w celu wykrycia i zlokalizowania, a następnie śledzenie toru przemieszczania się intruza/intruzów. Dowolnie konfigurowana maska obszarów chronionych/niechronionych w całej strefie działania pozwala na wyeliminowanie sygnałów nie objętych nadzorem.

Czujniki radarowe funkcjonują skutecznie na ziemi, wodzie i w powietrzu, w każdych warunkach pogodowych, a sposób oświetlenia nie ma na nie wpływu. Przy właściwym ustawieniu parametrów charakteryzują się wyjątkowo niskim współczynnikiem fałszywych alarmów.

W obserwowanym obszarze wykrywają one czołgające się, idące lub biegnące osoby, a także pojazdy, łodzie, znajdujące się na ziemi samoloty i wszystkie inne poruszające się obiekty. Dodatkowo do ich zalet, w przypadku zastosowania w systemach ochrony, zaliczyć należy:
- możliwą współpracę z GPS w celu dokładnej lokalizacji czujników radarowych w terenie,
- umożliwienie integracji radaru z innymi systemami ochrony, np. do sterowania kamerami w celu oceny zagrożenia przez operatora,
- możliwość identyfikacji zagrożenia przez operatora i optymalnego zaplanowania reakcji,
- szybką reakcję (reakcja jest możliwa w ciągu sekund, nie minut),
- brak konieczności śledzenia monitorów przez operatora, dopóki radar nie sygnalizuje alarmu,

– wysoką rozdzielczość: radar pracujący na wyższej częstotliwości i z węższą wiązką będzie określał pozycję intruza dokładniej.

Do podstawowych parametrów technicznych radarów perymetrycznych należy zaliczyć:

– częstotliwość pracy **od pasma X (około 10 GHz) do pasma W (około 77 GHz)**;
– typ modulacji (CW, FMCW i impulsowa); systemy z modulacją FMCW typowo mają bardzo dużą rozdzielczość (często większą niż 1m);
– zakres pracy **od 300 metrów do 10 km**;
– metody detekcji: dopplerowska i mapowanie;
– częstotliwość skanowania przestrzeni: od 360° na sekundę do 30° na sekundę (niektóre radary dopplerowskie mogą mieć mniejszą częstotliwość skanowania).

Dlaczego warto stosować radar w zabezpieczeniach?

– działa w każdych warunkach atmosferycznych w dzień i w nocy,
– jest bardzo trudny do ominięcia,
– ma duży zasięg i 360-stopniowe pokrycie terenu,
– umożliwia zabezpieczenie dużych obszarów przy zastosowaniu sieci,
– pozwala na oszacowanie zagrożenia dzięki ciągłemu śledzeniu celu,
– charakteryzuje się niskimi kosztami i dużą szybkością instalacji,
– może być stosowany tam, gdzie inne czujniki nie są praktyczne (np. nad wodą),
– programowalne strefy alarmowe pozwalają na dynamiczną zmianę obszaru detekcji.

Radary i rozwój technologii sensorów falowych

W klasycznym systemie ochrony, w którym do rozmieszczenia wymienionych we wstępie czujników na obwodzie chronionego obiektu konieczna jest budowa obwodnicy – pasa ziemi o szerokości co najmniej 3 m między dwoma ogrodzeniami, zewnętrznym i wewnętrznym – obowiązuje równocześnie wizualna weryfikacja alarmów, co wymusza stosowanie nadzoru wizyjnego w postaci kamer wizyjnych dzienno-nocnych do obserwacji liniowej obwodnicy i sprzężenie tych systemów ze sobą za pomocą odpowiedniego oprogramowania. Efektywna obserwacja nocna wymusza stosowanie oświetlenia lampowego obwodnicy. Całość systemu wymaga też budowy kanalizacji kablowej wzdłuż obwodnicy, co najmniej dwururowej (zasilanie, sygnały alarmowe, wizja, sieć telekomunikacyjna systemu), w celu wizualizowania sytuacji alarmowych w Centrum Nadzoru. W sumie uzbrojona, aktywna obwodnica z Centrum Nadzoru mieszczącym urządzenia końcowe systemów zastosowanych na obwodnicy to pracochłonne i drogie przedsięwzięcie inżynieryjne z poważnymi robotami ziemnymi.

Wydarzenia ostatnich lat, począwszy od 11 września 2001 r., a później wojny irackiej i afgańskiej, konieczność ochrony obozów wojskowych, konwojów i patroli oraz kolejne akty terrorystyczne w Madrycie i Londynie przyspieszyły rozwój systemów ochrony infrastruktury krytycznej zarówno w zakresie technologii czujników, modernizacji systemów i poglądów dotyczących organizacji skutecznej ochrony dostosowanej do również rosnących możliwości i umiejętności grup terrorystycznych i przestępczych.

Do stosowanej od ponad 20 lat kamery wizyjnej z matrycą CCD, wykrywającej promieniowanie widzialne odbite od obiektu, dołącza na przełomie wieku znacznie tańsza kamera termowizyjna, wykorzystująca matrycę bolometryczną (nie chłodzoną). Detekcja kontrastu termicznego obiektu na tle sceny uniezależnia zestaw kamery wizyjnej i termowizyjnej od oświetlenia sceny, co zwiększa w istotny sposób prawdopodobieństwo wykrycia obiektu zarówno w dzień, jak i w nocy, a także jego rozpoznania i identyfikacji. Mimo wszystko taki zestaw kamerowy jako element biernej obserwacji jest podatny na wpływy atmosferyczne (np. mgła posiada cząsteczki wody rezonujące z promieniowaniem podczerwieni w paśmie 3–5 μm, a zatem skutecznie tłumi to pasmo podczerwieni).

W celu zwiększenia skuteczności sensorów falowych w zakresie nadzoru wizyjnego wprowadzono radar naziemny w zakresie fal mikrofalowych o zasięgu 3–10 km i fal milimetrowych o zasięgu do 3 km. Trzy pasma falowe (mikrofale, podczerwień i zakres promieniowania widzialnego) przy aktywnym trybie pracy pasma radarowego uzupełniają się wzajemnie, a **zestaw sensorowy jako całość uniezależnia się zarówno od zmian dobowych, pogodowych i maskowania intruza**, np. termicznego. Ponadto zestaw ten spełnia podstawową zasadę detekcji intruza – zasadę podwójnej technologii detekcji aktywnej i pasywnej.

Drugim niezmiernie ważnym aspektem rozwoju systemów falowych jest rozwój metod analizy obrazu, prowadzący w konsekwencji do automatycznej detekcji intruza, wypracowanie sytuacji alarmowej i automatycznego śledzenia ruchu intruza. Aktualnie stosowane systemy wizyjne są wyposażone lub doposażone (zewnętrznie) w urządzenia automatycznej analizy obrazu (*Intelligent Vision* lub *Automatic Video Surveillance*). Automatyczna analiza obrazu jest bardziej efektywna niż praca operatora, a przy systemie rozbudowanym wręcz niezastąpiona. Ostatnim osiągnięciem tej informatycznej technologii jest fuzja, czyli **łączenie obrazów oraz informacji uzyskanych z zastosowanych trzech technologii (kamer wizyjnych, termowizyjnych oraz radarów) w jeden obraz *(Image Fusion[1])***. Rozwiązanie to ma umożliwić stosowanie jednego ekranu z jednym obrazem złożonym z wydatnych cech obrazu pojedynczych wizji termo i radaru milimetrowego. Tak określone **kierunki rozwoju technicznego zewnętrznych systemów ochrony zapowiadają dominację technik falowych – telewizji dozorowej, termowizji i technik radarowych – w najbliższych latach**.

DR INŻ. MAREK ŻYCZKOWSKI
LABORATORIUM SYSTEMÓW BEZPIECZEŃSTWA I ANALIZY ZAGROŻEŃ
INSTYTUT OPTOELEKTRONIKI
WOJSKOWA AKADEMIA TECHNICZNA ,
IM. JAROSŁAWA DĄBROWSKIEGO W WARSZAWIE

Literatura:

1. G. Hamman, *Perimeter surveillance radar system training session*, STS, czerwiec 2004.
2. *Perimeter surveillance radar system*, Manual, STS.
3. NATO NIAG SG 109 Technical Documents.
4. General Security – Navtech Radar – materiały firmowe.
5. ADMIR i MINDER firmy Elta – materiały firmowe.
6. SOWA firmy RADWAR – materiały firmowe.

1) Aktualnie technologia Image Fusion nie jest jeszcze stosowana w systemach dostępnych na rynku.

Ochrona zewnętrzna domu i posesji

W dzisiejszych czasach, w których stale rośnie wskaźnik przestępczości, system sygnalizacji włamania i napadu (SSWiN) stał się elementem koniecznym każdego domu, mieszkania czy obiektu komercyjnego. Coraz bardziej wyrafinowane systemy alarmowe w znaczący sposób zwiększają bezpieczeństwo osób i mienia. Rozwój elektronicznych systemów gwarantuje coraz większą skuteczność wykrywania i wysoką odporność na występowanie fałszywych alarmów. Z biegiem lat stają się one coraz bardziej ogólnodostępne. Na pewno przekłada się to w znaczący sposób na spadek liczby przestępstw mających największe znaczenie dla poczucia bezpieczeństwa społeczeństvwa, a mianowicie kradzieży i włamań. Poziom tego typu przestępstw jest jednak wciąż dość wysoki i, jak wynika ze statystyk policyjnych, codziennie 70 domów, mieszkań i domków letniskowych w Polsce pada ofiarą kradzieży z włamaniem

Wraz z rozwojem systemów sygnalizacji włamania i napadu wzrastają również oczekiwania klientów końcowych. To z jednej strony sprzyja edukacji osób odpowiedzialnych za sprzedaż i instalację, a z drugiej generuje coraz ciekawsze rozwiązania wprowadzane przez producentów, którzy prześcigają się, aby sprostać stawianym oczekiwaniom.

W niniejszym artykule chciałbym skupić się na zagadnieniach związanych z ochroną zewnętrzną, która staje się coraz bardziej popularna także w przypadku domów i posesji. Od dawna dostępne są systemy ochrony perymetrycznej wykorzystujące różne zjawiska fizyczne. Niegdyś były to przede wszystkim systemy powstające na potrzeby wojska, które następnie były adaptowane do zastosowań komercyjnych. Znacząca większość tych systemów powstała do ochrony rozległych obiektów, takich jak bazy wojskowe czy granice państw. Ze względu na środowisko stosowania i sposób instalacji systemy ochrony zewnętrznej możemy podzielić jak niżej.

1. Systemy ogrodzeniowe instalowane na wewnętrznym ogrodzeniu obwodnicy:
- a) kablowe tryboelektryczne,
- b) kablowe mikrofonowe,
- c) kablowe światłowodowe natężeniowe i interferometryczne,
- d) kablowe elektromagnetyczne,
- e) czujniki piezoelektryczne punktowe,
- f) ogrodzenie aktywne – z wmontowanymi czujnikami mechaniczno-elektrycznymi.

2. Systemy naziemne:
- a) aktywne bariery mikrofalowe,
- b) aktywne bariery podczerwieni,
- c) pasywne czujki podczerwieni,
- d) dualne czujki PIR/MW
- e) radary mikrofalowe,
- f) radary laserowe.

3. Systemy ziemne:

a) kablowe elektryczne aktywne (pole elektryczne),
b) kablowe magnetyczne pasywne (pole magnetyczne),
c) kablowe światłowodowe naciskowe,
d) kablowe elektromagnetyczne naciskowe,
e) czujniki sejsmiczne.

Wymienione systemy są szeroko wykorzystywane w obiektach militarnych, ochrony lotnisk czy granic. Każde rozwiązanie ma swoje wady i zalety. Co więcej, systemy ochrony zewnętrznej ze względu na ciężkie warunki pracy są systemami bardzo złożonymi technicznie, często trudnymi w instalacji oraz dość drogimi. Są to czynniki, które wielu użytkowników i instalatorów odstraszają.

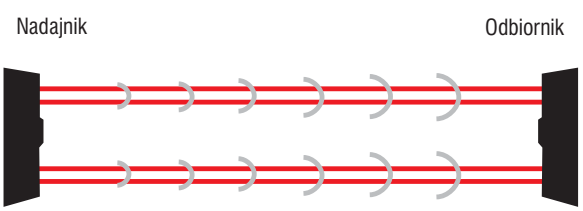
Ze względu na trudne warunki pracy i w celu ograniczenia występowania fałszywych alarmów z reguły stosuje się dwa zewnętrzne systemy ostrzegawcze – system ogrodzeniowy i naziemny lub ziemny. Dodatkowo sprzęga się je z systemem telewizji dozorowej w celu weryfikacji alarmu. Takie rozwiązanie ochrony zewnętrznej jest zwykle stosowane do ochrony obiektów specjalnych. Na potrzeby ochrony zewnętrznej standardowej posesji czy domku jednorodzinnego stosuje się sprawdzone i przeznaczone do tego typu obiektów rozwiązania; są to głównie systemy naziemne. Najszerzej stosowane z nich to kolejno:

– czujki dualne PIR/MW,
– aktywne bariery podczerwieni,
– pasywne czujki podczerwieni,
– aktywne bariery mikrofalowe.

Poniżej zostaną omówione najbardziej popularne rozwiązania, czyli czujki ruchu oraz bariery podczerwieni.

Aktywne bariery podczerwieni

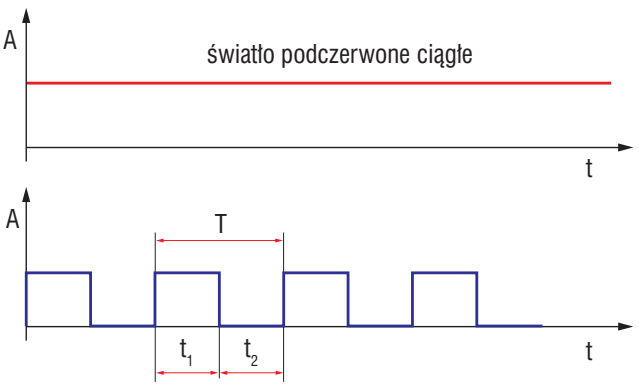
Aktywne bariery podczerwieni składają się z co najmniej dwóch urządzeń: nadajnika i odbiornika, zainstalowanych naprzeciw siebie. W nadajniku jest wbudowana dioda elektroluminescencyjna (LED – GaAlAs) emitująca podczerwień z zakresu 0,85–0,95 μm.



Rys. 1. Rzut boczny czterowiązkowej bariery podczerwieni ilustrujący zasadę działania urządzenia

Każdy nadajnik posiada wbudowany układ optyczny, za pomocą którego ogniskuje wiązkę podczerwieni na powierzchnię odbiornika. W odbiorniku znajduje się fotodioda krzemowa typu p-i-n. Ze względu na duże natężenie promieniowania LED oraz niewielką powierzchnię światłoczułą diody stosuje się specjalne układy optyczne zwiększające powierzchnię odbioru. W związku z tym zwiększa się również moc promieniowania padającego na powierzchnię fotodiody. Układy te stanowią również filtr optyczny mający na celu uodpornienie bariery na zakłócenia, takie jak oświetlenie światłem słonecznym lub próba oślepienia (np. latarką).

Bardzo ważnym elementem jest również stosowanie w barierach szyfrowania i zapisywania w odbiorniku charakterystyki nadawanego sygnału z nadajnika. Stosuje się syntetyczną modulację impulsową, która jest charakterystyczna dla konkretnego nadajnika i odbiornika. Odbiornik porównuje sygnał odebrany w postaci ciągu impulsów z zapisanym sygnałem wzorcowym od „swojego" nadajnika. Uniemożliwia to ingerencję osób postronnych, chcących obejść system przez oświetlenie odbiornika promieniami podczerwonymi.



Rys. 2. Rozwiązanie tradycyjne oraz sygnał impulsowy wykorzystywany w rozwiązaniach Bosch zwiększających odporność na fałszywe alarmy (A – amplituda, t_1 – czas trwania impulsu, t_2 – czas przerwy impulsu, T – okres)

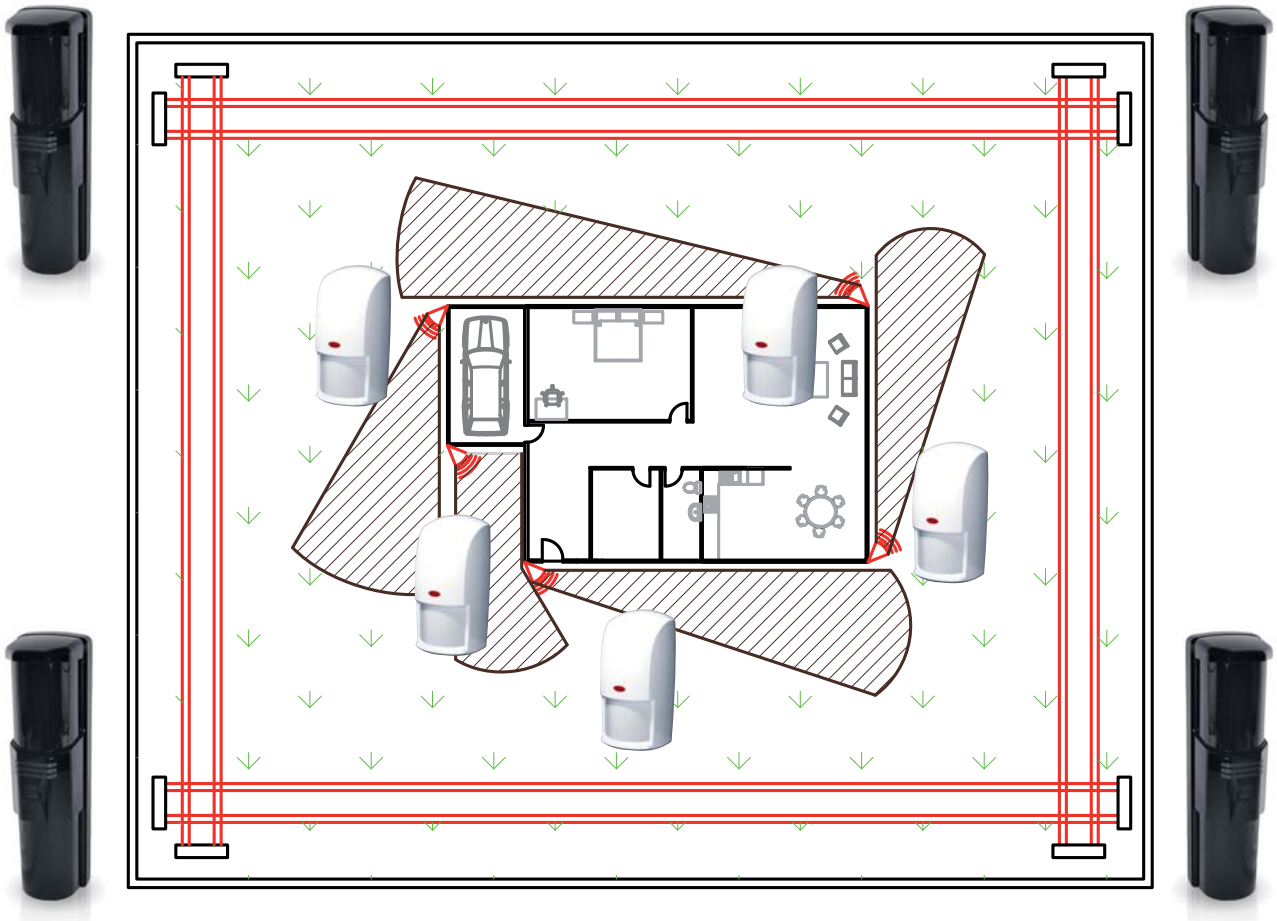
Przy projektowaniu i instalacji barier podczerwieni należy zapewnić ich niezakłóconą pracę. Działanie tych urządzeń może być zakłócone przez rosnące krzaki, drzewa czy wysoką trawę, a także warunki atmosferyczne, np. mgłę, która może w znaczący sposób absorbować promieniowanie podczerwieni. Należy ściśle przestrzegać następujących reguł:

– nadajnik i odbiornik zawsze muszą się „widzieć" (na linii nadajnik – odbiornik musi być zapewniona widoczność, niezakłócona przez roślinność, nierówności terenu czy inne obiekty),
– bariery muszą być przystosowane do pracy w warunkach zewnętrznych,
– należy przestrzegać określonych w instrukcji maksymalnych odległości między nadajnikiem i odbiornikiem, aby zapewnić niezakłóconą pracę barier,
– nie należy montować nadajnika narażonego na bezpośrednie oślepienie przez inne źródła światła,
– w przypadku braku szyfrowania należy unikać krzyżowania się wiązek, które w przypadku zgodnych faz mogą wzbudzać fałszywy alarm.

Specyfika działania aktywnych barier podczerwieni jest obszernym tematem, jednak rozumiejąc ich sposób funkcjonowania oraz przestrzegając wyżej wymienionych reguł można z powodzeniem zaprojektować skuteczny system z wykorzystaniem tych urządzeń.

Czujki zewnętrzne

Najpowszechniej stosowanymi czujkami do ochrony wewnętrznej są pasywne czujki podczerwieni (PIR czyli PCP) oraz czujki zespolone – PIR z czujnikiem mikrofalowym, które są również wykorzystywane do zastosowań zewnętrznych. Ze względu na bardzo ciężkie warunki pracy czujki zewnętrzne, choć bazują na tych samych zależnościach fizycznych, są o wiele bardziej zaawansowanymi urządzeniami. W przypadku ochrony zewnętrznej zaleca się stosowanie czujek dualnych pracujących w trybie AND, czyli wywołujących alarm na podstawie informacji z obu detektorów – PIR i MW (mikrofala).



Rys. 3. Sposób rozmieszczenia barier podczerwieni w przykładowym projekcie

Wielu producentów wprowadza na rynek czujki zewnętrzne PIR, często z poczwórnym piroelementem, polecane i chwalone przez instalatorów. Czujki te są zaawansowane technologicznie i gwarantują minimalizację występowania fałszywych alarmów. Posiadają funkcję analizy sygnału, są odpowiednio uszczelnione i przystosowane. Natomiast w przypadku pracy w trudnym środowisku zewnętrznym czujki powinny mieć bardzo dużą tolerancję warunków pracy. Dlatego czujka generująca alarm na podstawie informacji uzyskanej tylko z torów PIR, w zastosowaniach, w których muszą być tolerowane podmuchy powietrza, zmiany temperatur, odbijające oświetlenie czy drobne zwierzęta, będzie bardzo zawodna. Wielu producentów chwali się, że oferowane przez nich zewnętrzne czujki PIR są odporne na zwierzęta domowe. W takiej sytuacji warto się zastanowić, czy czujki, które generują alarm, wykorzystując tylko pasywną podczerwień, i mają dużą tolerancję w odniesieniu do różnych warunków pracy, będą reagowały właściwie, gdy intruzem będzie niewysoki człowiek.

Z tym tokiem rozumowania nie wszyscy muszą się zgodzić, natomiast pewne jest to, że im więcej informacji w systemach ochrony jest poddanych analizie, tym system jest skuteczniejszy. W przypadku zastosowania do ochrony zewnętrznej czujki dualnej alarm jest generowany w wyniku wykorzystania dwóch niezależnych technologii.

Przy wyborze czujki ważne jest, aby była ona wykonana z jak najlepszych materiałów, gdyż musi funkcjonować w silnym nasłonecznieniu, jak również w niskich temperaturach. Takie warunki pracy sprzyjają zmęczeniu materiału. Ważnym elementem jest optyka, która, jak wcześniej wspomniano, oprócz zadania ogniskowania promieniowania podczerwieni na piroelemencie pełni również rolę filtra. W nowoczesnych czujkach stosuje się zaawansowane technologie przetwarzania sygnałów PIR i mikrofali, wykorzystujące różne parametry.

Aby zapewnić stabilną i efektywną pracę czujki, należy zwrócić uwagę na takie czynniki, jak:

- **miejsce umieszczenia czujki** – takie, aby czujka była skuteczna; powinna być zamontowana jak pułapka, należy przewidzieć ewentualne miejsca wtargnięcia intruza, aby w sposób maksymalny wykorzystać właściwości detektora;
- **wysokość instalacji** – zgodna z instrukcją instalacji, taka, aby nie powstawały martwe strefy;
- **rodzaj podłoża** – instalacja powinna zostać wykonana na stabilnym podłożu;
- **eliminacja** (o ile to możliwe) **źródeł fałszywych alarmów**, takich jak bezpośrednie oślepianie czujki czy wentylatora powietrza; mimo odporności na niesprzyjające warunki nie należy niepotrzebnie obciążać procesora czujki;
- **wzajemna ochrona** – czujki powinny być skierowane w tym samym kierunku, aby każda kolejna czujka „patrzyła" na tył następnej i chroniła przed nieuprawnionym podejściem z boku detektora;
- **ustawienia i regulacja obszaru chronionego** (przydatny jest do tego tzw. walk test);
- **odpowiedni montaż** przewodów, puszek itp.

Przykładowe rozwiązanie zabezpieczenia zewnętrznego domku jednorodzinnego

Nie istnieją algorytmy, na bazie których można byłoby zaproponować najlepszy i najskuteczniejszy system bezpieczeństwa. Do każdego obiektu należy podchodzić indywidualnie, aby uniknąć popadnięcia w rutynę. Proces projektowania można natomiast podzielić na kolejne fazy, które w większości inwestycji należy wykonać:

- **I faza**: doradztwo (analiza zagrożeń, a następnie analiza słabych punktów, analiza ryzyka);
- **II faza**: planowanie systemu – koncepcja i wstępny kosztorys, alternatywne rozwiązania, ocena, wybór wariantu, opracowanie koncepcji systemu;
- **III faza**: projektowanie – konfiguracja systemu, planowanie szczegółów (montaż, materiały, instalacja, uruchomienie, szkolenie, harmonogram prac), projekt techniczny, kosztorysy, termin realizacji;
- **IV faza**: realizacja i uruchomienie systemu – dostawa, montaż, uruchomienie, szkolenie, dokumentacja powykonawcza;
- **V faza**: obsługa systemu – praca systemu, konserwacja i serwis systemu, dozór obiektu.

Mając na uwadze przedstawiony powyżej sposób postępowania, chciałbym przedstawić praktyczne zastosowanie wcześniej omówionych urządzeń w przypadku zabezpieczania przykładowego domu jednorodzinnego usytuowanego na działce o kształcie prostokąta i wymiarach 60 m x 50 m. Przeprowadzona analiza funkcjonalna i czynnikowa wykazała wysoki stopień zagrożenia działaniami przestępczymi. Działka ogrodzona jest płotem z siatki metalowej o wysokości 2 m. Zdecydowano się na zaprojektowanie ochrony zewnętrznej bazującej na aktywnych barierach podczerwieni DS484Q oraz zewnętrznych czujkach dualnych OD850 firmy Bosch.

Projekt rozmieszczenia barier podczerwieni został przedstawiony na rys. 3. Są to czterowiązkowe bariery przystosowane do pracy w warunkach zewnętrznych. Ich olbrzymią zaletą jest możliwość ustawienia pracy AND lub OR, czyli wywołanie alarmu może być spowodowane przecięciem wszystkich czterech wiązek albo też dwóch górnych lub dwóch dolnych wiązek. Bariery Bosch są wyposażone również w obwód dyskryminatora czynników środowiskowych. Monitorują stopniową utratę sygnału spowodowaną kurzem, mgłą, śniegiem, deszczem itp., odpowiednio nadzorując i automatycznie regulując wzmocnienie wiązki. Gwarantuje to poprawną pracę nawet w skrajnie niekorzystnych warunkach. Specjalne wyjście typu NC zmienia swój stan, gdy utrata sygnału wynosi 90%. Bariery umożliwiają również pracę wielokanałową – do wyboru jest aż osiem różnych kanałów (osiem różnych częstotliwości wiązki). Pozwala to na korzystanie z wielu barier zainstalowanych blisko siebie przy eliminacji ryzyka interferencji i wystąpienia fałszywego alarmu. Konstrukcja barier została zaprojektowana w taki sposób, aby maksymalnie ułatwić instalację i zestrojenie barier dzięki wbudowanej diodzie sygnalizacyjnej LED alarmu, wewnętrznej diodzie LED zasilania nadajnika, diodzie LED poziomu zestrojenia, wyjścia napięciowego oraz sygnalizatora dźwiękowego w odbiorniku.

Do bezpośredniej ochrony obiektu zastosowano zewnętrzne czujki dualne OD850, które zostały już sprawdzone na polskim rynku i są idealnym rozwiązaniem do tego typu obiektów. Montaż czujek został dokonany z uwzględnieniem fizycznego obrysu budynku, przez co osiągnięto pełne pokrycie obszaru wokół chronionego obiektu. Czujki OD850 cechuje przede wszystkim najwyższa jakość zastosowanych materiałów oraz inteligentna analiza sygnałów PIR za pomocą technologii ***Motion Analyzer II***. Sygnały mikrofalowe są analizowane dzięki technologii **LTD** ***(Linear Travel Distance)***. Dzięki temu detektory są w stanie odróżnić małe, powtarzające się ruchy, np. kołysanie się drzew na wietrze, od ruchu intruza.

Dzięki technologii *Motion Analyzer II* uaktywnienie alarmu następuje w wyniku analiz taktowania, amplitudy, czasu trwania i polaryzacji sygnału, wykonywanych przy użyciu różnych progów i okien czasowych detektora PIR. Dzięki temu ekstremalnie wysokie lub niskie temperatury spowodowane podmuchami gorącego i zimnego powietrza, zaburzenia oświetlenia promieniami słonecznymi czy wyładowania atmosferyczne nie powodują generowania fałszywych alarmów.

Istotą technologii LTD jest przetwarzanie sygnału mikrofalowego przez mikroprocesor, który podejmuje decyzję o wygenerowaniu alarmu na podstawie pomiaru długości przemieszczenia liniowego celu. Zapobiega to wywoływaniu alarmu przez obiekty, które wprawdzie się poruszają, ale nie przemieszczają, takie jak gałęzie drzew czy wiszące szyldy. Dodatkowo istnieje możliwość regulacji czułości detektora PIR w zależności od środowiska pracy czujek.

Tak szczegółowa i zaawansowana obróbka sygnału oznacza, że czujki posiadają wbudowaną „inteligencję" i dzięki temu są w stanie odróżnić właściwe zagrożenia od źródeł fałszywych alarmów. Co więcej, czujki są bardzo uniwersalne i można je stosować właściwie w każdym typie obiektu.

Podsumowanie

Dobrze zaprojektowany system ochrony obiektu powinien tak funkcjonować, aby czas sforsowania zabezpieczeń mechanicznych przez intruza był dłuższy od sumarycznego czasu zadziałania systemu sygnalizacji alarmu i dotarcia załóg interwencyjnych.

System ochrony zewnętrznej w znaczący sposób podnosi wartość zainstalowanego systemu oraz skraca czas wczesnego wykrycia, co zwiększa możliwość reakcji, zanim intruz wyrządzi szkody. Do zalet stosowania ochrony zewnętrznej w obiekcie nie trzeba nikogo przekonywać. Oczywiście, jak każde rozwiązanie, ma ono również sporo wad, ale, jak wiadomo, nie ma rozwiązań idealnych. Wskazówki, które zostały przedstawione w artykule, na pewno będą pomocne przy wyborze odpowiednich urządzeń, a zawarte w nim sugestie mogą pomóc przy proponowaniu konkretnego rozwiązania.

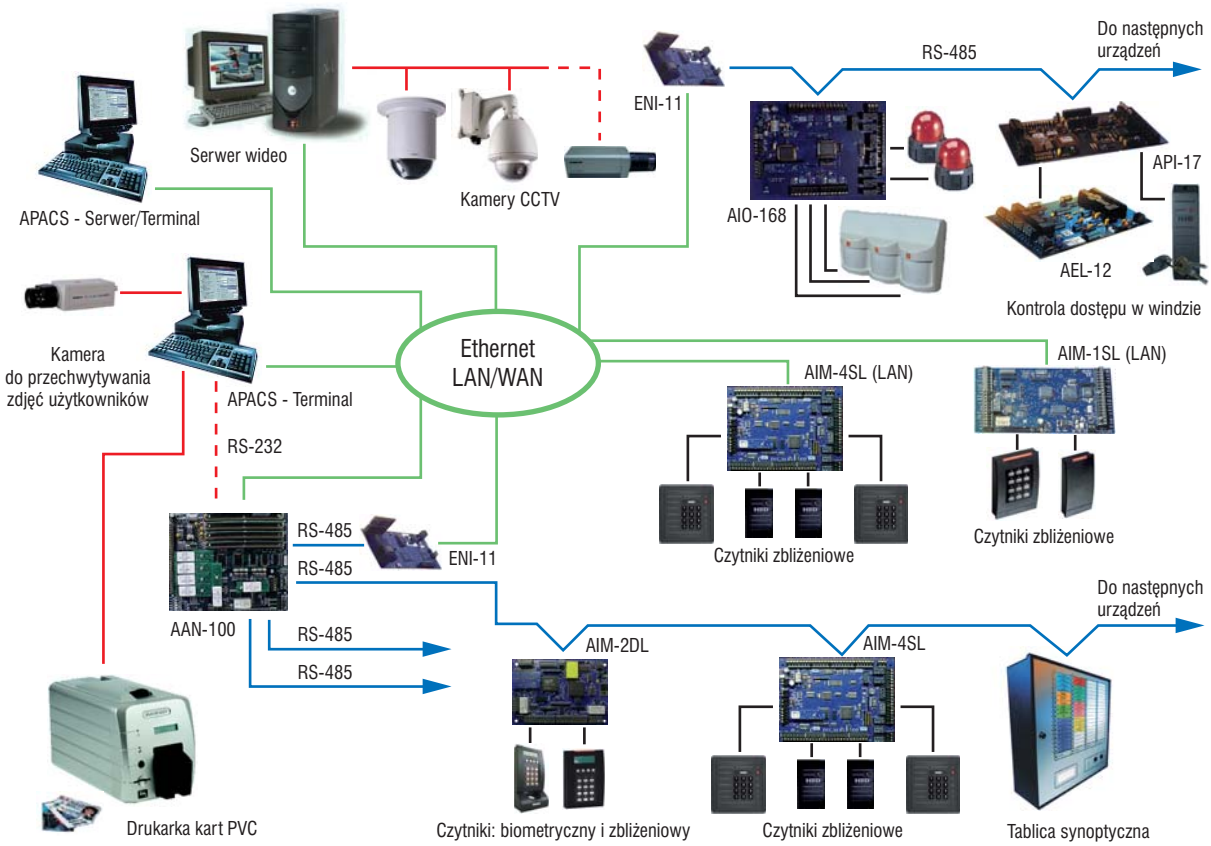
Należy pamiętać, że system bezpieczeństwa to nie tylko elektroniczne systemy ostrzegawcze, ale również zabezpieczenia mechaniczne, wprowadzone procedury i zasady dla użytkowników obiektu oraz ich świadomość jako integralnej części systemu bezpieczeństwa.

W artykule zostały przedstawione w ogólny sposób pewne zasady i reguły, jakimi należy się kierować przy projektowaniu, doborze urządzeń i instalacji. Jednak wszystkie te elementy nie zastąpią profesjonalnych szkoleń z tej dziedziny, organizowanych przez różne instytucje. Zapraszamy do odwiedzenia naszej strony internetowej www.boschsecurity.pl oraz do udziału w organizowanych przez nas bezpłatnych szkoleniach, dotyczących produktów z pełnej oferty rynku systemów zabezpieczeń.

Krzysztof Kostecki
Bosch Security Systems

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.

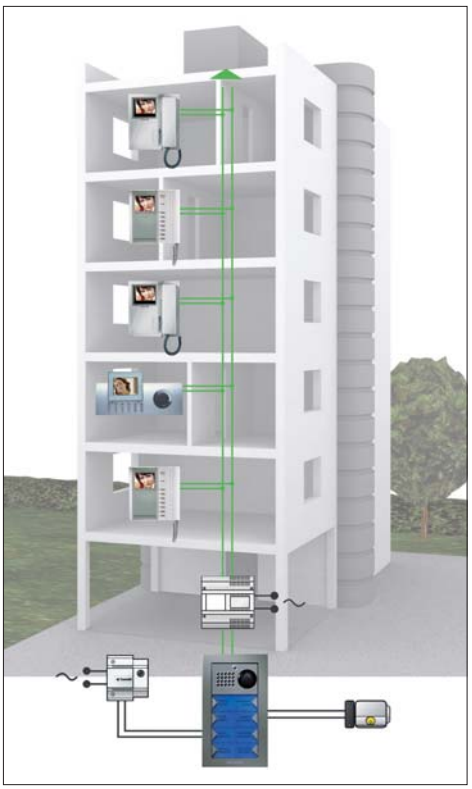


- 32 stacje robocze
- 32 kontrolery główne (AAN)
- 3072 czytniki
- 16 384 linie alarmowe
- 8192 wyjścia przekaźnikowe
- 79 000 zdarzeń off-line (w standardzie)
- 100 dni świątecznych
- 127 stref czasowych (6 przedziałów w każdej strefie)
- 256 poziomów dostępu
- Równoległa obsługa do 8 formatów kart
- 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.

Aparaty wewnętrzne dostępne w systemie Simplebus Color

GENIUS

BRAVO

DIVA

UNIFON STYLE

Panele wejściowe

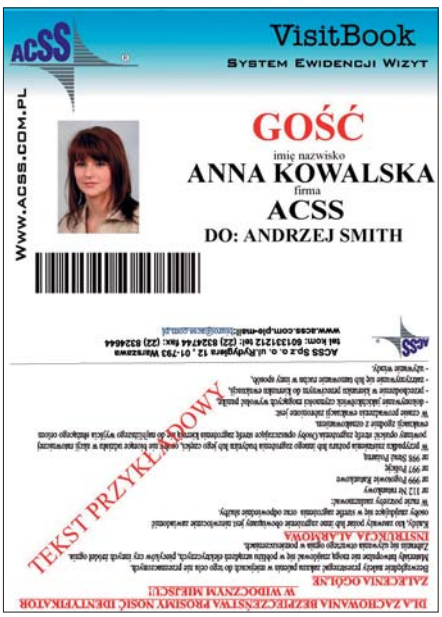
W systemie Simplebus2 można zastosować panele wejściowe serii Powercom jak i wandaloodporne Vandalcom. Oba panele występują w wersji cyfrowej z elektronicznym spisem nazwisk oraz z indywidualnymi przyciskami wywołania. Ramki zewnętrzne paneli dostępne są w różnych kolorach.

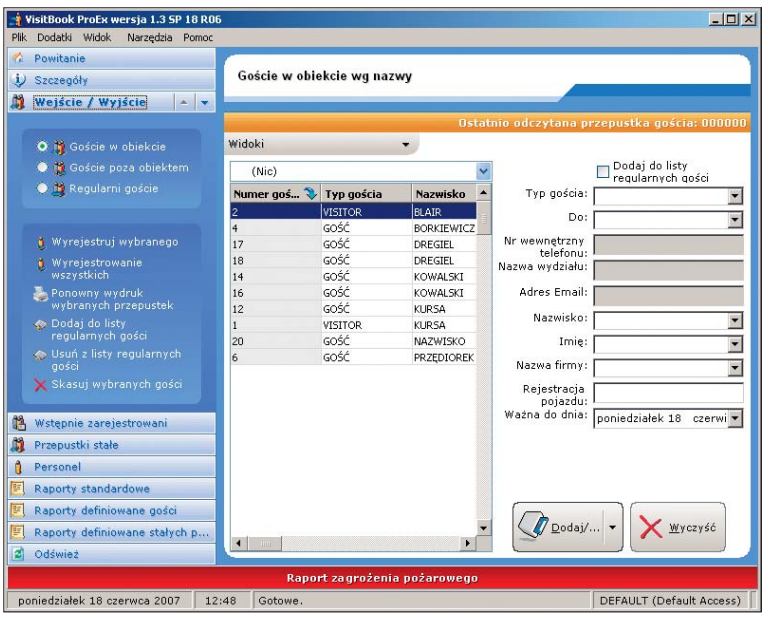
alarmnet®

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

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

System 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

Modułowa drukarka do kart identyfikacyjnych PVC

Enduro™
MAGICARD

MAGICARD holo Kote

HoloKote™ - znak wodny drukowany na całej powierzchni karty. Widoczny przy patrzeniu pod kątem. 4 wzory do wyboru.

Full Bleed

Nadruk od krawędzi do krawędzi z jakością 300 dpi.

holo patch

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

Mag stripe

Możliwość kodowania pasków magnetycznych(opcja).

Duplex printing

Dwustronny nadruk (opcja).

Taśmy kolorowe:
– 250 kart (nadruk dwustronny)
– 300 kart (nadruk jednostronny)
Taśmy monochromatyczne nadruk 1000 kart.
Kolory taśm monochromatycznych:
czarny, czerwony, niebieski, zielony,
złoty, srebrny i biały.

Drukarka jednostronna z możliwością rozbudowy do wersji dwustronnej

Specyfikacja techniczna
Prędkość nadruku
– Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund – Monochromatyczny wydruk karty w 4,5 sekundy (przy specyficznych warunkach)
Cykl działania
– Ciągły
Wbudowane zabezpieczenia
– HoloKote™ anty-coping – znak wodny na całej powierzchni karty. Wybór jednego z 4 wzorów
Typ taśmy
– MA300YMCKO: YMCKO nadruk 300 kart – MA250YMCKOK: nadruk dwustronny 250 kart (przód kolor, tył czarny) – MA1000K: Monochromatyczny nadruk 1000 kart – MA600KO: Monochromatyczny nadruk (czarny i overlay) 600 kart
Rodzaje
– **Enduro** jednostronna drukarka do kart z możliwością upgradu do wersji dwustronnej – **Enduro Duo** dwustronna drukarka do kart
Karty
– Drukuje na wszystkich standardowych kartach PCV ISO CR80 o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych – Dostępne karty z HoloPatch™
Pobór karty
– Automatyczny z podajnika lub podawanie ręczne
Pojemność magazynków kart
– Podajnik 100 kart – Zasobnik kart nadrukowanych 30 sztuk
Głowica
– 300 dpi (wymienna)
Interfejs do PC
– USB rev. 1.1. (kompatybilny z USB 2.0)
Sterowniki (w języku polskim)
– Windows 2000, 2003 Server user-mode, XP, VISTA
Kompatybilność elektromagnetyczna i certyfikat
– EN 50 081-1 i EN 50 082-1 (Europa)/CE
Zasilanie
– 90-265 V / 47-63 Hz
Wymiary / Waga
– 453 mm x 206 mm x 233 mm / 5,5 kg
Temperatura pracy
– od 10°C do 30°C
Gwarancja
– 2 lata

ACSS

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

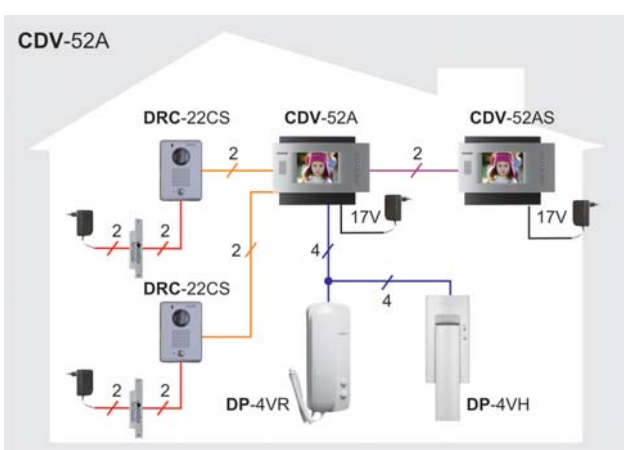
tel. (22) 832 47 44, faks (22) 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl, http://www.magicard.com.pl

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

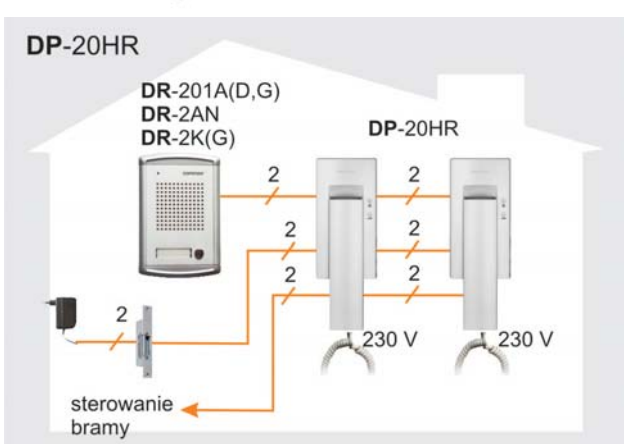
Domofon DP-20HR / DR-2***

DP-20HR uzupełnia ofertę firmy GDE Polska o kolorowe unifony dla prostych systemów jednorodzinnych. Unifon występuje w pięciu wersjach kolorystycznych obudowy, dzięki czemu klient może dostosować urządzenie do kolorystyki wnętrza mieszkania. Unifon posiada dodatkowy przycisk umożliwiający np. otwieranie elektrycznie sterowanej bramy. **DP-20HR** może współpracować z dowolną stacją bramową serii **DR-2*****.

Wszystkie domofony firmy Commax charakteryzują się bardzo prostą instalacją (do komunikacji pomiędzy unifonem a stacją bramową wystarczą 2 żyły, dodatkowe 2 żyły do obwodu elektrozamka), wysoką jakością wykonania, niezawodnością oraz nowoczesnym wzornictwem. Cechy te sprawiają, że są one chętnie wybierane przez osoby poszukujące prostego systemu do komunikacji z furtką wejściową.

Produkty współpracujące:

DR-201A DR-201D DR-2AN DR-2G DR-2K DR-201AG DR-2A2N DR-2A3N



Specyfikacja techniczna	
Okablowanie	2 przewody
Zasilanie	AC 100-240 V 50/60 Hz
Pobór prądu	maks. 150 mA
Temperatura pracy	0 - 40°C
Wymiary (szer. / wys. / gł.):	94 mm x 258 mm x 54 mm
Masa:	600 g

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 cyfrowy Falcon DD04100 V

Falcon DD04100 V to nowy rejestrator w ofercie firmy Factor Security. Ma on możliwość nagrywania 4 kamer z prędkością 100 kl/s, w kompresji MPEG4. Rejestrator może realizować sześć procesów jednocześnie (tzw. sextaplex), czyli nagrywanie, podgląd na żywo, odtwarzanie, archiwizacja, sterowanie, dostęp zdalny. Oprócz standardowego wyjścia monitorowego typu BNC posiada także dodatkowe wyjście VGA do podłączenia monitora komputerowego. Do rejestracji obrazu z podłączonych kamer urządzenie używa dysku twardego o pojemności do 500 GB, natomiast do archiwizacji może być użyty czytnik kart SD oraz port usb, do którego możemy podłączyć wszelkie urządzenia zapisujące. Rejestrator posiada możliwość podglądu i konfiguracji poprzez sieć LAN. Ciekawą funkcją jest możliwość wysyłania e-maili z informacjami o zdarzeniach alarmowych typu utrata sygnału, detekcja ruchu czy naruszenie wejścia alarmowego i możliwość zgrywania tych zdarzeń na serwer FTP. Porty RS485/422 i RS232 pozwalają na sterowanie rejestratorem z wyniesionej klawiatury sterującej jak i sterowanie kamerami ruchomymi z samego rejestratora. Istnieje także możliwość podłączenia do portów RS modemu GPS lub systemu POS w celu zapisywania danych z obrazem nagrywanym z kamer.

Specyfikacja techniczna		
Wideo	Format Wejścia wideo Monitor główny Monitor pomocniczy	PAL/CCIR 4-CH, BNC BNC x 2, S-wideo x 1, VGA x 1 BNC x 1
Audio	Wejście / Wyjście	2 / 2, RCA-jack
Nagrywanie	Kompresja Prędkość zapisu / Rozdzielczość Znak wodny Opcje nagrywania Pre-record Post-record	MPEG-4 Advanced Simple Profile (ASP) PAL - 25 / 720x576, 50 / 720x288, 100 / 352x288 tak ręczne /według kalendarza / alarmowe / z detekcji ruchu 0 - 10 s 0 - 60 min
Wyświetlanie	Rozdzielczość Podział ekranu Prędkość wyświetlania	PAL - 720x576 1/4 25 kl./s
Odtwarzanie	Prędkość / Rozdzielczość Wyszukiwanie	PAL - 25 / 720x576, 50 / 720x288, 100 / 352x288 data/czas, kamera, alarm, ruch
Zapis	Dyski twarde Archiwizacja	1 x 500 GB 1 x czytnik kart SD, 1 x USB 2.0 dla podłączenia zewnętrznych dysków USB, czytników kart itp.
Alarm	Wejścia / Wyjścia Naruszenie	4 / 1 czujnik, utrata sygnału, detekcja ruchu
Sieć LAN	Ethernet WWW E-mail FTP Dostęp	1 RJ-45 10/100BaseT zdalne programowanie, monitoring, przegląd alarmów informacja o zdarzeniach alarmowych zapis plików alarmowych 6 użytkowników jednocześnie
Sterowanie	I/R RS-232 RS-485/422	1 x pilot IR (opcjonalnie) 1 D-type, sterowanie kamerami ruchomymi 1 D-type, do podłączenia klawiatury sterującej
Programowanie	Lokalne Zdalne	przez panel przedni, pilota IR lub klawiaturę sterującą przez sieć LAN za pomocą dołączonego oprogramowania
Zabezpieczenia	System Filtr przeciwpyłowy Hasła	automatyczne uruchomienie po utracie zasilania tak wielopoziomowy system haseł
Wymiary / Masa	Wymiary Masa	215 (szer.) x 260 (gł.) x 72 (wys.) mm 2.8 kg (bez HDD)
Zasilanie	Źródło Pobór mocy	90~264 V AC, 47~63 Hz 18 W maks.

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

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

STID-ACIE
ul. Poleczki 21
02-822 Warszawa
tel./faks (22) 894 61 63
e-mail: info@acie.pl
www.acie.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 41 A
01-755 Warszawa
tel. (22) 633 90 90
faks (22) 633 90 60
e-mail: info@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. Komisji Edukacji Narodowej 96 Lok. U15
02-777 Warszawa
tel. (22) 855 00 17÷19
faks (22) 546 19 78
e-mail: cs@cs.pl
www.cs.pl, www.ckp.com.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. Gliwicka 3
40-079 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85
e-mail: dravisdravis@neostrada.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

Plac Jana Pawła II 82i, 66-400 **Gorzów Wielkopolski**
tel. (95) 722 12 12
tel./faks (95) 722 12 14
e-mail: factor.go@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

Przedsiębiorstwo Usług Technicznych INTEL 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

SAWEL SYSTEMY BEZPIECZEŃSTWA
ul. Lwowska 83
35-301 Rzeszów
tel. (17) 857 80 60, 857 79 80
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

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

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 17/14
faks (74) 847 00 69
e-mail: walbrzych@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

CENTRUM SYSTEMÓW ZABEZPIECZEŃ

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. Stefana Batorego 28-32
81-366 **Gdynia**
tel. (58) 782 00 00
faks (58) 782 00 22

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

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

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

TECHOM

Zakład Rozwoju Technicznej Ochrony Mienia TECHOM Sp. z o.o.

– Centrum Kształcenia Zawodowego Instalatorów i Projektantów Systemów Alarmowych, Monitoringu oraz Rzeczoznawstwa

– Laboratorium Badawcze Elektronicznych Urządzeń Alarmowych

ul. Marszałkowska 60
00-545 Warszawa
tel. (22) 625 34 00
faks (22) 625 26 75
e-mail: techom@techom.com
www.techom.com

TECHNOKABEL
łączy i przewodzi

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

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

Tri-Kon

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 & Integrated Solutions

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.
GRUPA FIRM UNICARD

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

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

Visonic Central Europe
For a smart and secure lifestyle

VISONIC Sp. z o.o.
ul. Smoleńskiego 2
01-698 Warszawa
tel. (22) 639 34 36, 37
faks (22) 833 48 60
e-mail: visonic@visonic.com.pl
www.visonic.com.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
ACIE	TAK	-	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	-	-
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	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

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Intel	-	TAK	TAK	TAK	TAK
Ired	TAK	TAK	TAK	TAK	-
Janex International	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	-	TAK	-	TAK	-
Kolektor MR	-	TAK	TAK	TAK	-
Krak-Poż	-	TAK	-	TAK	-
Laskomex	TAK	TAK	TAK	TAK	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	-	-	-	-
Sawel	-	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
Visonic	-	-	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	-	-
ACIE	-	-	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	-
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

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
Intel	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
Ired	TAK	TAK	TAK	-	-	TAK	TAK	-	-
Janex International	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Krak-Poż	-	-	-	TAK	-	-	TAK	-	TAK
Laskomex	-	TAK	TAK	-	-	-	TAK	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	-	-
Sawel	TAK	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
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	TAK	-	-	-	-	-	-	-	-
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	-	-	-	-	-
Visonic	TAK	-	TAK	-	-	-	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:
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
Krzysztof Białek
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:

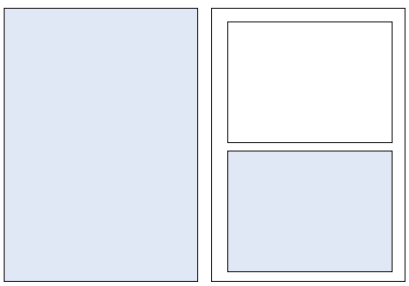
jednorazowy wpis	70 zł

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji

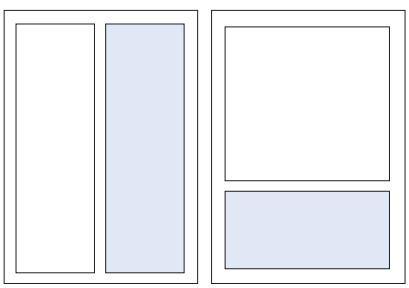
W przypadku zamówienia na 12 emisji 10% rabat

Podane ceny nie uwzględniają podatku VAT (22%)

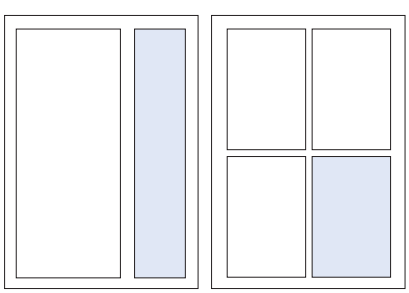
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej **http://www.zabezpieczenia.com.pl** w dziale **Reklama**



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

IndigoVision

KOMPLETNE ROZWIĄZANIE VIDEO IP

MONITORING MIEJSKI
MONITORING STADIONÓW
MONITORING DWORCÓW I LOTNISK

MEPG-4 H.264 PoE HD-RES

System IndigoVision to wysokiej jakości system bezpieczeństwa video IP, posiadający cechy tradycyjnych systemów CCTV, takich jak: zapis na rejestratorach autonomicznych, funkcje krosownicy, możliwość podłączania analogowych monitorów, zarządzanie funkcjami wyświetlania oraz sterowania PTZ za pomocą sprzętowego sterownika z joystickiem. Encodery oraz kamery IP IndigoVision charakteryzują się bardzo wysoką jakością obrazu przy zachowaniu stosunkowo małych strumieni danych,

System IndigoVision dedykowany jest zarówno do małych instalacji wykorzystujących infrastrukturę sieci komputerowej (w tym również sieci bezprzewodowej) np.: monitoring w małych miastach, monitoring firm, osiedli, jak również do dużych systemów instalowanych w portach lotniczych, na stadionach, autostradach czy w dużych wielotysięcznych miastach. System IndigoVision dysponuje szerokim zakresem analizy obrazu. Dzięki czemu za pomocą oprogramowania można zautomatyzować obserwację, wykorzystując takie funkcje jak detekcję ruchu, śledzenie obiektu, wykrywanie tłoku oraz pozostawionych przedmiotów. Dzięki funkcji integracji z innymi systemami bezpieczeństwa (np.: kontrola dostępu), system IndigoVision jest jednym z najlepszych w swojej klasie i może być stosowany w obiektach o najwyższym poziomie ochrony.

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

IndigoVision Authorized Partner

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.