CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(58)2007

ZABEZPIECZENIA

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

W NUMERZE:

5 grzechów głównych nowych kamer URMET

Elastyczność

1092/200
Kamera dzień&noc 550 linii
w trybie kolor; min. czułość 0 lux
(przy wł. IR-Led); mech. filtr IR;
obiektyw asferyczny 3,8-9,5mm/DC;
wbudowane diody (zasięg 15m/30°);
IP65; zas. 12 Vdc

Elastyczność

Profesjonalizm

1090/110
Kamera WDR dzień&noc 480 linii
w trybie kolor; min. czułość
0,001 lux/F1,2 (przy wł. DSS);
mech. filtr IR; OSD, RS-485;
Lina-Lock; zas. 230 Vac

Profesjonalizm

Inteligencja

1092/650 Easy Dome II
Kamera EX-VIEW dzień&noc
z funkcją **auto-tracking,**
zintegrowana w głowicy szybkoobrotowej;
480 linii w trybie kolor; min. czułość 0,01 lux;
mech. filtr IR; obiektyw x 26 zoom (3,5-91mm),
x 12 zoom cyfrowy; 256 presetów,
prędkość do 400 °/s (w trybie auto),
8 stref prywatności; 4 wej. / 2 wyj. alarmowe.

Inteligencja

Perfekcja

1092/160-161
Kamera dzień&noc 550 linii
w trybie kolor; min. czułość 0,008 lux/F1,2
(przy wł. DSS); mech. filtr IR;
SDNR-system redukcji szumów;
SuperDSS x32;
1092/160 zas. 12 V dc,
1092/161 zas. 230 V ac.

Perfekcja

Zaufanie

1092/103-104
Kamera kolorowa 540 linii;
min. czułość 0,5 lux/F1,2;
elektroniczna funkcja dzień&noc
(tryb monochrom. nieczuły na IR);
ATW/AWB;
1092/103 zas. 12Vdc/ 24Vac (Line-Lock),
1092/104 zas. 230 Vac (Line-Lock).

Zaufanie

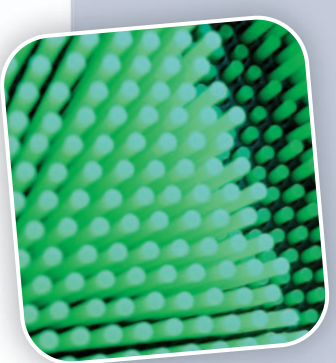
MIWI-URMET Sp. z o. o.
91-341 Łódź, ul. Pojezierska 90 A
tel. (042) 616 21 00, fax (042) 616 21 13
www.miwiurmet.com.pl
e-mail: miwi@miwiurmet.com.pl

urmet MIWI

CZASOPISMO ZABEZPIECZENIA 6/2007

w numerze

22
Aspekty monitorowania bezpieczeństwa wewnątrz dużych instytucji finansowych



32
Nie bójmy się biometrii!

50
exacqVision – hybrydowy system nadzoru wizyjnego do kamer analogowych i kamer IP

64
HDP5000 – nowa drukarka Fargo

XI Walne Zgromadzenie PIOOiM

W dniach 27–28 września 2007 r. w ośrodku wypoczynkowym FWP w Spale odbyło się **XI Walne Zgromadzenie Polskiej Izby Ochrony Osób i Mienia (PIOOiM)**, w którym udział wzięło 75 przedstawicieli firm członkowskich, dysponujących na podstawie upoważnień 91 mandatami.

Wśród zaproszonych gości byli przedstawiciele Krajowej Izby Gospodarczej, Polskiej Konfederacji Pracodawców Prywatnych „Lewiatan", Komendy Głównej Policji, Unii Polskich Organizacji Branży Ochrony, Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm", Polskiego Związku Pracodawców „Ochrona", Polskiej Izby Systemów Alarmowych oraz delegacja czeska jako lider Klubu Europejskich Organizacji Branży Ochrony „ESBOC", przewodzący Klubowi w tym roku.

PIOOiM, jako organizacja samorządu gospodarczego, aktualnie reprezentuje interesy 218 przedsiębiorców branży ochrony, detektywistyki i tzw. obrotu specjalnego, prowadzących działalność usługową, produkcyjną, handlową oraz w zakresie szkolnictwa.

Izba od 13 lat spełnia istotną rolę w systemie bezpieczeństwa wewnętrznego. Instytucje naszego państwa postrzegają Izbę jako naturalnego partnera oraz ważne „ogniwo w łańcuchu bezpieczeństwa" kraju.

XI Walne Zgromadzenie Polskiej Izby Ochrony Osób i Mienia, które 28 września 2007 roku zakończyło dwudniowe obrady, dokonało oceny dwuletniej działalności zarządu Izby oraz zaktualizowało kierunki działań Izby, ustalone na X Walnym Zgromadzeniu we wrześniu 2005 r., na kolejne dwa lata.

Zebrani wyrazili wolę rozwijania przez Izbę procesu integracji przedsiębiorstw branżowych ze względu na rozwój rynku krajowego i rynków zagranicznych w zakresie usług, głównie ochrony osób i mienia.

Izba będzie udzielała pomocy i wspierała firmy członkowskie w zakresie zwiększania konkurencyjności przedsiębiorstw oraz podnoszenia jakości produktów i świadczonych usług.

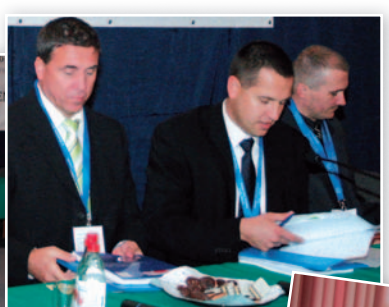
W zakresie regulacji prawnych uznano za bardzo ważne monitorowanie i aktywną współpracę z organami władzy i administracji w zakresie zmian przepisów prawnych dotyczących branży ochrony.

Dokonano zmiany statutu Izby i regulaminu działania jej organów.

Podjęta została decyzja o wzmacnianiu regionalnych programów współpracy na rzecz bezpieczeństwa z działającymi w tym obszarze instytucjami samorządowymi oraz administracją państwową.

XI Walne Zgromadzenie zaakceptowało powołanie przez zarząd Izby Fundacji Pomocy Pracownikom Ochrony i Ich Rodzinom „Ochrona i Pomoc".

W XI Walnym Zgromadzeniu uczestniczyli również liczni wystawcy, prezentując swoje wyroby i usługi:
AMZ – Kutno – pojazdy specjalne,
Brokerzy i Konsultanci – ubezpieczenia,
CSO Magazyn Zarządzających Bezpieczeństwem – wydawnictwo,
Inter Graw Marek Gralewski – systemy komputerowe,
Krajowa Izba Rozliczeniowa – archiwizacja dokumentów,
Kwantor – sprzęt łącznościowy,
Nexum Brokerzy Ubezpieczeniowi – ubezpieczenia,
Nostra – filmowe materiały szkoleniowe,
Nowatex – odzież robocza,
Radmor – sprzęt łącznościowy,
Signella – 1 A i S Staszewscy – pojazdy specjalne,
Spółdzielnia Pracy Wyrobów Skórzanych im. J. Kilińskiego – obuwie,
Tasc Technology – sprzęt elektroniczny,
TestDNA Polska – testery DNA.



Zenon Parchimowicz
dyrektor biura zarządu
Polskiej Izby Ochrony
Osób i Mienia

XII edycja konkursu Polski Mistrz Techniki Alarmowej 2008

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm" zaprasza polskich oraz zagranicznych producentów i dystrybutorów elektronicznych i elektromechanicznych urządzeń oraz systemów przeznaczonych do ochrony osób i mienia do udziału w XII edycji konkursu **„Polski Mistrz Techniki Alarmowej 2008"**.

Konkurs będzie przeprowadzony w następujących kategoriach przedmiotowych:

I Urządzenia i systemy sygnalizacji włamania i napadu
II Urządzenia i systemy sygnalizacji pożaru
III Urządzenia i systemy nadzoru telewizyjnego i rejestracji obrazów
IV Urządzenia i systemy kontroli dostępu
V Zintegrowane systemy sygnalizacji zagrożeń
VI Urządzenia i systemy transmisji alarmu oraz monitoringu
VII Systemy zabezpieczenia przeciwkradzieżowego pojazdów
VIII Systemy zarządzania i bezpieczeństwa transportu
IX Systemy zarządzania i bezpieczeństwa ładunków
X Inne urządzenia i systemy technicznej ochrony oraz wspomagające ochronę fizyczną

Zgłoszenia do udziału w konkursie będą przyjmowane **do dnia 27 lutego 2008 roku,** na drukach „Wniosku o udział w konkursie", które prosimy przesłać na adres biura zarządu stowarzyszenia Polalarm: ul. Nowogrodzka 18/8, 00-511 Warszawa, e-mail: polalarm@polalarm.com.pl lub polalarm@alter.pl.

Ogłoszenie wyników konkursu i uroczystość wręczenia nagród laureatom odbędzie się w pierwszym dniu Międzynarodowej Wystawy Zabezpieczeń „Securex 2008" **w Poznaniu, tj. 22 kwietnia 2008 r.**

Regulamin konkursu i wniosek o udział w konkursie dostępne są w na stronie www.polalarm.com.pl oraz w biurze zarządu stowarzyszenia Polalarm w Warszawie, przy ul. Nowogrodzkiej 18/8, tel./faks **(0-22) 625-57-43, 626-90-31.**

Serdecznie zapraszamy do udziału w konkursie i życzymy sukcesów!

Bezpośr. inf. Polalarm

Prewencja 14–16 marca 2008 IV Targi Zabezpieczeń i Ochrony Mienia w Szczecinie

Zeszłoroczna edycja targów pokazała, że wciąż poszukujemy nowych rozwiązań z zakresu zabezpieczeń. Podczas kolejnej, czwartej już edycji targów zaprezentowane zostaną m.in. najnowsze trendy i rozwiązania z zakresu elektronicznych i mechanicznych systemów zabezpieczeń oraz zabezpieczania i ochrony danych, a także sprzęt i odzież specjalistyczna, pojazdy specjalistyczne i sprzęt do samoobrony. Odbędą się kursy samoobrony. Oferowane będą usługi ochrony i nadzoru, a także ubezpieczenia z zakresu ochrony i nadzoru oraz zabezpieczenia mienia i osób.

Kolejna edycja będzie towarzyszyła, jak w roku ubiegłym, Międzynarodowym Targom Budowlanym „BUD-GRYF" – największej i najliczniejszej pod względem liczby wystawców i odwiedzających imprezie targowej w regionie.

Zapraszamy Państwa do udziału w targach.

Marzena Piotrowska
komisarz MTS
Międzynarodowe Targi Szczecińskie
tel.: +48 91 464 44 01, faks: +48 91 464 44 02
http://www.mts.pl

securex 2008 POLAND

Wysokiej klasy bezpieczeństwo

Coraz większa świadomość polskiego społeczeństwa dotycząca konieczności i rosnących możliwości zwiększenia poziomu bezpieczeństwa poprzez zastosowanie systemów alarmowych, kontroli dostępu, monitoringu itp. sprawia, że branża zabezpieczeń rozwija się bardzo dynamicznie. Wraz z nią ewoluuje także **Międzynarodowa Wystawa Zabezpieczeń „Securex"**. Jej najbliższa edycja odbędzie się w dniach **22–25 kwietnia 2008 roku w Poznaniu.**

Securex 2008 zapowiada się bardzo interesująco. Już teraz sygnały docierające z branży pozwalają przewidywać, że grupa wystawców będzie jeszcze liczniejsza, a program tematyczny bogatszy niż ostatnio. – *Staramy się, aby Securex był szerokim polem wymiany doświadczeń, a także miejscem odkrywania nowych możliwości* – podkreśla **Bartosz Zeidler**, **dyrektor Securexu**. – *Przyszłoroczna edycja przyniesie kilka niespodzianek – wśród nich atrakcyjne wydarzenie dla profesjonalistów z branży, a także obecność nowych, dotychczas niespotykanych na targach grup docelowych. Szczegóły pozostają na razie tajemnicą.* Ponadto, już tradycyjnie, odbędzie się wręczenie nagród w konkursie **„Polski Mistrz Techniki Alarmowej"**, organizowanym przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **„Polalarm"**. To oczywiście nie wszystko – prace nad programem trwają, a organizatorzy są otwarci na wszelkie sugestie – np. zagadnienia dotyczące problematyki zapewnienia poziomu bezpieczeństwa podczas Euro 2012.

Targi Securex gromadzą producentów i dystrybutorów, projektantów i wykonawców, liderów rynku oraz małe i średnie firmy, dając kompleksowy przegląd ofert w zakresie nowoczesnych technologii zabezpieczania mienia, dostępnych na rynku polskim i zagranicznym. Ponadto wystawcy w jednym miejscu mają dostęp do szerokiego grona odbiorców: architektów, projektantów instalacji, instalatorów i wykonawców, deweloperów, przedstawicieli służb ochrony banków, muzeów, sieci handlowych i hotelarskich, służb publicznych oraz pracowników zajmujących się w przedsiębiorstwach ochroną mienia i ludzi.

Decyzja o rezygnacji z corocznej organizacji targów była niełatwa, lecz spotkała się z pełną aprobatą uczestników. Spojrzenie na statystykę targów Securex 2006 to potwierdza: wzrost liczby wystawców o 48%, wzrost powierzchni zajętej przez ekspozycję o 80% oraz wzrost liczby zwiedzających – odbywające się jednocześnie targi Securex, Sawo, Instalacje i Aqua San w 2006 roku odwiedziło blisko 24500 zwiedzających z 25 krajów. Tym, co przyciąga do Poznania najbardziej, jest chęć zapoznania się z innowacjami, a tych było na ostatnich targach Securex ponad 100.

Nadchodząca edycja zapowiada się naprawdę ciekawie. Organizatorzy na razie nie chcą zdradzić wszystkiego, ale jedno jest pewne – będzie bezpiecznie. W końcu jedziemy na Securex!

Bezpośr. inf. MTP

Targi A+A 2007 Podsumowanie

W dniach 18-21 września 2007 roku odbyły się w Düsseldorfie (Niemcy) Międzynarodowe Targi Bezpieczeństwa i Higieny Pracy, Środków Ochrony Indywidualnej i Bezpieczeństwa w Zakładzie Pracy „A+A 2007" (edycja 27).

W porównaniu z poprzednią edycją targów sprzed dwóch lat wzrosła liczba uczestników tej imprezy (z 54350 do 55100). Udział wzięło 1460 wystawców z 51 krajów. Równolegle odbywający się kongres A+A zarejestrował ok. 6000 uczestników. Przyjęli oni bardzo dobrze piętnaście tłumaczonych symultanicznie sesji warsztatowych na temat bezpieczeństwa i higieny pracy.

Można śmiało powiedzieć, że bezpieczeństwo pracy rozwinęło się z marginesowej dziedziny do nowoczesnej dyscypliny, obecnej w łańcuchu procesów biznesowych, na co zwrócił uwagę Eugen Müller – przewodniczący niemieckiej Federalnej Grupy Roboczej ds. Bezpieczeństwa i Higieny Pracy Basi . (*Bundesarbeitsgemeinschaft für Sicherheit und Gesundheit bei der Arbeit*), organizatora kongresu. O tym, że targi A+A służą za wskaźnik trendów w dziedzinie bezpieczeństwa na rynku europejskim świadczy fakt, że ponad 20% gości przybyło nad Ren z zagranicy.

Wystawcy zaprezentowali kompletne spektrum produktów i usług, służących do ochrony osobistej, zapewnienia bezpieczeństwa zbiorowego i promocji higieny w miejscu pracy - począwszy od przedmiotów służących do zabezpieczania poszczególnych części ciała oraz wyposażenia dla służb ratowniczych, aż do urządzeń do ochrony przeciwpożarowej i zagadnień związanych z projektowaniem ergonomicznych mebli do biur. Na uwagę zasługuje m.in. urządzenie diagnostyczne z biologicznym sprzężeniem zwrotnym, służące do badania naprężeń mięśni wywoływanych przez nieprawidłową pozycję podczas wykonywania pracy. Innymi przykładami innowacyjnych rozwiązań były: nowoczesne ekrany do redukcji hałasu w otwartych przestrzeniach biurowych, kabiny dla palaczy z efektywnymi wyciągami dymu, kamery termiczne, służące do wykrywania ukrytych źródeł pożaru.

Duże wrażenie wywarł spektakularny projekt badawczy Niemieckiego Stowarzyszenia Promocji Ochrony Przeciwpożarowej VFDB (*Vereinigung zur Förderung des Deutschen Brandschutzes*), a zwłaszcza unoszący się podczas targów nad jednym ze stanowisk sześciometrowej długości bezzałogowy sterowiec. Był on wyposażony w odpowiednie urządzenia pomiarowe, umożliwiające zdalną ocenę zagrożeń (np. zanieczyszczeń powietrza lub stężenia gazów szkodliwych) na podstawie przesyłanych drogą radiową do centrum kontrolnego obrazów oraz wyników pomiarów.

Następne targi A+A odbędą się w Düsseldorfie w dniach 3-6 listopada 2009 r.

Redakcja
Źródło: Messe Düsseldorf

ST4EX – więcej niż przenośny czytnik biometryczny

Trijay Technologies International Corporation (TTI), we współpracy z firmą Smart Media Innovations (SMI), stworzyła **ST4EX** – wielofunkcyjne urządzenie przenośne (terminal), łączące w sobie zalety telefonu komórkowego oraz palmtopa ze zintegrowanym biometrycznym czytnikiem, umożliwiającym zdalne uwierzytelnianie. Inaczej mówiąc, jest to miniaturowy, przenośny komputer (zawierający system operacyjny z dodatkowymi aplikacjami), który umożliwia zdalne (przez GSM/GPRS) podłączenie się do rożnych systemów informatycznych, np. podsystemów kontroli dostępu firmy, zasobów wymagających uwierzytelnienia itp. Obszary jego zastosowań ograniczone są tylko ludzką wyobraźnią – urządzenie można wykorzystać np. do zarządzania systemami bezpieczeństwa, w służbie zdrowia (do zdalnego odczytu historii choroby lub wyników badań), w wyborach parlamentarnych, w bankowości (przelewy, dyspozycje bankowe), w sklepie (robiąc zakupy), w agencjach rządowych, wojsku, na lotniskach. Może być ono także wykorzystane przez służby graniczne i policję (potwierdzanie rozkazów, zadań, korzystanie z baz danych, sprawdzanie/potwierdzanie tożsamości pasażera posiadającego paszport biometryczny – uzyskujemy funkcjonalność biometrycznego terminala lotniskowego, tzw. kiosku).

ST4EX umożliwia zdalne uwierzytelnianie z wykorzystaniem biometrycznego czytnika linii papilarnych oraz różnych formatów bezstykowych kart identyfikacyjnych RFID, elektronicznego paszportu z krojem pisma OCR-B oraz kodów kreskowych 1D i 2D.

Wyjątkowość rozwiązania polega na zintegrowaniu wielu systemów – chodzi tu o wykorzystywanie różnych formatów kart chipowych, paszportu, dowodu biometrycznego z RFID – i uzyskaniu mocnego uwierzytelnienia (można jednoznacznie określić autentyczność paszportu, jednoznacznie dopasować dokument do jego właściciela i np. skierować pytanie o niekaralność do KRS). Funkcjonalność urządzenia jest ogromna w stosunku do jego wielkości, a nie zapominajmy o tym, że jest to komputer, czyli zrobi wszystko, co nakaże aplikacja – można wprowadzić do jego pamięci lokalizacje GPS, potraktować urządzenie jako modem, punkt dostępowy itp.

Urządzenie posiada kolorowy monitor dotykowy wielkości 3,5", klawiaturę numeryczną, moduł GSM/GPRS oraz moduły RFID (Mifare, HID iCLASS), gniazda do kart SIM i SAM, czytnik kart SD, biometryczny czytnik linii papilarnych oraz skaner optyczny (OCR-B) np. do czytania pasków MRZ paszportów i kodów kreskowych 1D i 2D. Umożliwia bezprzewodowy dostęp do sieci Ethernet (WLAN) i komunikację szeregową oraz przez USB Bluetooth i poczerwień (IrDA).

Redakcja
Źródło: Trijay Technologies International Corporation (TTI)

Promocja Milestone Systems dla użytkowników kamer IP **Pelco**

Użytkownicy produkowanych przez Pelco kamer IP serii Camclosure IP mają możliwość zapoznania się z oprogramowaniem XProtect firmy Milestone Systems dzięki bezpłatnej licencji na oprogramowanie obsługujące jedną kamerę. Informacja o tej promocji firmy Milestone Systems znajduje się na stronie http://www.milestonesys.com/dk/pelco oraz na ulotce umieszczonej w pudełku z kamerą Pelco IP110/IP111. Kod promocji: PLFLY0906D5. Na mocy porozumienia zawartego z Pelco, Milestone Systems była pierwszą firmą na świecie, która zintegrowała produkty serii Camclosure IP ze swoim oprogramowaniem.

Bezpośr. inf. Pelco

Bezprzewodowa lustrzanka PIR Visonic PowerMax PRO

Dzięki wprowadzeniu na rynek nowej czujki **Tower**, system **PowerMax PRO**, przeznaczony dotąd głównie dla odbiorców prywatnych oraz małych biur, może być teraz stosowany także w obiektach przemysłowych. Jest to cyfrowa bezprzewodowa lustrzanka, zapewniająca perfekcyjną analizę badanego sygnału. Dzięki specjalnej podwójnej obudowie czujka jest bardziej odporna na wszelkie czynniki zewnętrzne, takie jak pył lub inne zanieczyszczenia unoszące się w powietrzu. Dodatkowe zabezpieczenia antysabotażowe uniemożliwiają zerwanie lub przesunięcie czujki bądź otwarcie jej obudowy. Docelową grupą odbiorców czujki Tower są firmy realizujące zabezpieczenia bezprzewodowe na rynku przemysłowym, w halach produkcyjnych lub innych pomieszczeniach, w których zagrożenie wystąpienia niepożądanego alarmu jest relatywnie duże.

Bezpośr. inf. Visonic

SECURITY 2008

XV Międzynarodowe Targi Specjalistyczne oraz seminarium poświęcone bezpieczeństwu i ochronie

Termin: 12–15 lutego 2008 r.
Częstotliwość: impreza coroczna
Miejsce: Międzynarodowy Pałac Kultury, Sofia

Główne grupy produktów: urządzenia i systemy sygnalizacji włamania i napadu, kontroli dostępu, kontroli obwodowej (perymetrycznej), transmisji alarmów, telewizji dozorowej; sygnalizacji pożarowej i ochrony przeciwpożarowej, zarządzania budynkiem (BMS), szyfrowania i zapobiegania przechwytywaniu komunikacji, telekomunikacyjne, alarmy samochodowe i immobilizery, stacje monitoringu i pojazdy patrolowe, wyposażenie policyjne, urządzenia do ochrony osobistej, rozwiązania do ochrony danych i dokumentów oraz informacji niejawnych, wyposażenie ochronne banków, sejfy, pomieszczenia zabezpieczone przed włamaniem i pożarem (*strong rooms*), pojazdy opancerzone, hotelowe systemy bezpieczeństwa i systemy bezpieczeństwa społecznego, urządzenia sygnalizacyjne; rozwiązania zwiększające bezpieczeństwo ruchu drogowego, drzwi pancerne, metalowe i garażowe, bariery itd.

Godziny otwarcia: 10.00–19.00
Otwarte dla: gości targowych oraz publiczności
Opłaty za wstęp: wstęp bezpłatny
Menedżer projektu: Violeta Nikolova

Organizator: Bułgarska Izba Handlu i Przemysłu, Wydział Targów i Wystaw, ul. Iskar 9, 1058 Sofia, Bułgaria; tel.: (+359 2) 989 7240, 989 22 40, 987 26 31; tel./faks: (+359 2) 981 66 26; e-mail: fairs@bcci.bg; Internet: http://www.bcci.bg/fairs/security/

Redakcja
źródło: BCCI-Fairs

Nowości Pelco na targach w Las Vegas

Podczas targów **ASIS 2007**, które odbyły się w dniach 24–27 września w Las Vegas, firma **Pelco** pokazała wiele nowych produktów oraz wzbogacone wersje już sprzedawanych urządzeń. Najwięcej innowacji dotyczy Endury – systemu wykorzystującego transmisję wideo w sieciach IP. Niżej wymienione nowości trafią do sprzedaży w ciągu najbliższych kilku miesięcy. Więcej informacji wkrótce.

Endura Intelligent Video – to kolejny etap rozwoju koderów Endury. Na targach zostały zaprezentowane nowe inteligentne kodery wideo, realizujące funkcje analizy obrazu, takie jak: detekcja usuniętego obiektu, zliczanie obiektów, analiza kierunku ruchu, detekcja pozostawionego obiektu i inne.

Endura Mapping – to uzupełnienie systemu Endura umożliwiające tworzenie map obiektu. Pozwala ono na szybki dostęp do strumieni wideo poprzez mapę oraz wizualizację stanów wejść i wyjść alarmowych.

Endura WS5000 wersja 1.5 – to nowe oprogramowanie stacji roboczej systemu Endura. Zmieniony interfejs umożliwia szybką i intuicyjną obsługę systemu. Wprowadzono nowe funkcje, związane z obsługą inteligentnych koderów i map.

Endura Gateway & Transcoder – to nowy element systemu Endura, umożliwiający dostęp do systemu przez Internet, poprzez przeglądarkę internetową. Umożliwia podgląd strumieni wideo, przeglądanie nagranego materiału oraz wykonywanie funkcji administracyjnych. Transmisja wideo jest skalowalna; *„gateway"* dostosowuje jej parametry do przepustowości połączenia internetowego.

Endura Wireless – to seria nowych bezprzewodowych koderów i nadajników, które pozwolą rozszerzyć zasięg systemu Endura o miejsca, w których nie można położyć okablowania – między innymi parkingi, porty lotnicze, nabrzeża portowe, obiekty zabytkowe. Urządzenia zapewniają szybką transmisję wysokiej jakości sygnału wideo.

DX4500/DX4600 – to nowe rejestratory serii DX4000. Są urządzeniami ośmio- i szesnastokanałowymi, z dyskami o pojemnościach do 3 TB. Są idealne do stosowania w małych systemach CCTV. Oprogramowanie do zdalnego dostępu umożliwia jednoczesne nadzorowanie kilku urządzeń tej serii.

DX8100 wersja 1.1 – to nowa wersja popularnego w Polsce rejestratora. Zbudowany na platformie Microsoft XP, ma teraz dwa kanały audio w standardzie, obsługę technologii multicastingu przy zdalnym podglądzie wideo, a także nowe opcje przeglądania wideo, eksportu i wydruku nagranego materiału.

Camclosure IP – to rodzina kamer IP do zastosowań wewnętrznych lub zewnętrznych. Do wyboru są cztery rodzaje kamer – kolorowa, dzienno-nocna oraz wersje z szerokim zakresem dynamiki (WDR) – a także dwa rodzaje obiektywów: 3,0–9,5 mm oraz 9,0–22,0 mm. Obraz wideo (MJPEG) można oglądać przy użyciu standardowej przeglądarki internetowej. Camclosure IP może również pracować w systemie Endura, w którym rejestrowane i przeglądane są strumienie MPEG4 o rozdzielczości 4CIF przy 25 kl./s.

Bezpośr. inf. Pelco

Nowy lider na rynku oprogramowania IP

Firma **Netavis** powstała w 1986 roku na Węgrzech. W 2003 roku część działalności przeniesiono do Wiednia. Dziś Netavis jest czołowym dostawcą oprogramowania IP, nie tylko na rynkach austriackim i węgierskim, ale także m.in. w Serbii i Arabii Saudyjskiej. Firma realizowała projekty zarządzania strumieniami wideo nawet z 4500 kamer. Na całym świecie sprzedano już ponad 20000 licencji na oprogramowanie Netavis. Od niedawna rozwiązania firmy można nabyć także w Polsce.

Oprogramowanie do monitoringu wizyjnego Netavis zostało oparte na systemie operacyjnym Linux, co w porównaniu do rozwiązań konkurencyjnych, wykorzystujących system operacyjny Windows, znacząco zwiększa stabilność aplikacji. Proces instalacji przebiega w prosty sposób, a równocześnie z platformą systemową instalowany jest system monitoringu wizyjnego Netavis Observer. W trakcie instalacji system jest dostosowywany do możliwości sprzętowych serwera i w rezultacie instalowane są tylko niezbędne komponenty. Pomimo mnogości oferowanych funkcji oraz korzystnego sposobu licencjonowania Netavis zachowuje atrakcyjną cenę.

Dla firm, które nie są w pełni zadowolone z dotychczas stosowanego oprogramowania IP, firma Netavis przygotowała specjalną ofertę. Już teraz, wymieniając je na rozwiązanie Netavis, zapłacisz jedynie 50% ceny.

Partnerem Netavis Software w Polsce jest **Softex Data.**

Bezpośr. inf. Softex Data

Przed sezonem zimowym

Długie, zimowe noce stanowią trudny test dla systemów telewizji dozorowej, które muszą sprawdzać się w warunkach niskiego poziomu oświetlenia. Część z nich nie zda egzaminu, ponieważ nie będzie w stanie dostarczyć nocnych obrazów wysokiej jakości.

Mając to na uwadze, Raytec stworzył *CCTV Lighting Pack* – zestaw informacyjny dostępny dla instalatorów, konsultantów oraz użytkowników, zawierający przewodnik po zagadnieniach, dotyczących oświetlenia w systemach telewizji dozorowej, płytę DVD oraz narzędzie zwane kalkulatorem cięcia kosztów. Materiały te pokazują najlepsze praktyki oraz technologie w dziedzinie oświetlenia światłem podczerwonym oraz białym, a ich celem jest zwiększenie wydajności systemów telewizji dozorowej w sezonie zimowym oraz ograniczenie kosztów ich stosowania i eksploatacji.

– Właściwe oświetlenie to istotny element systemu telewizji dozorowej przez cały rok, ale podczas długich zimowych nocy staje się ono warunkiem krytycznym. Okres ten jest najlepszym momentem do oceny działania takiego systemu i poczynienia w razie konieczności poprawek. Oprócz zestawu informacyjnego oferujemy bezpłatne konsultacje dotyczące istniejących oraz planowanych instalacji – powiedział David Lambert z firmy **Raytec.**

Redakcja
Źródło: Raytec

Nowe kamery Vivotek

Kamera **Vivotek IP 7151** i jej wersja bezprzewodowa **IP7152** są wyposażone w przetwornik CCD z progresywnym skanowaniem, dzięki któremu uzyskano wysoką jakość obrazu wideo w sam raz do profesjonalnego monitoringu w bankach, na lotniskach, parkingach, w kontroli ruchu drogowego itp. Kamery IP7151/IP7152 generują ostry, czysty i wysokiej rozdzielczości obraz poruszających się obiektów, jaki nie jest możliwy do uzyskania w tradycyjnej technologii skanowania międzyliniowego. Ponadto posiadają mechaniczny filtr IR, dzięki któremu, w połączeniu z bardzo czułym przetwornikiem CCD Vivotek, mogą dostarczać wysokiej jakości obrazy nawet przy minimalnym oświetleniu.

Do przetwarzania obrazu użyto nowoczesnego procesora WTK-1000 SoC Vivotek, dzięki któremu kamery IP7151/IP7152 mogą pracować w trybie *dual streaming* – udostępniać dwa niezależne strumienie wideo, np. jeden (wysokiej jakości) do archiwizacji, a drugi (dopasowany do zdalnego monitoringu) w wąskim paśmie przepustowości.

Nowe kamery posiadają także wiele udogodnień, które pozwalają użytkownikowi na większą elastyczność: zasilanie PoE (IP7151), wielojęzyczny interfejs użytkownika, możliwość wymiany obiektywów typu DC z mocowaniem CS, dwukierunkową transmisję dźwięku*), wejścia/wyjścia alarmowe.

Nowe kamery Vivotek IP7151 IP7152 to zdecydowanie najlepszy wybór do budowy niezawodnego systemu monitoringu wideo.

Oto ich cechy charakterystyczne:
- przetwornik CCD o rozdzielczości VGA,
- obiektyw zmiennoogniskowy 2,9÷8,2 mm z automatyczną przesłoną w komplecie,
- mechaniczny filtr IR,
- kompresja MPEG-4 i MJPEG (*dual codec*),
- tryb *dual streaming,*
- wbudowane zasilaniePoE (IP7151),
- wbudowany interfejs bezprzewodowej sieci Ethernet 802.11 b/g – WiFi (IP7152),
- dwukierunkowa transmisja dźwięku*),
- wejścia/wyjścia alarmowe,
- dołączone bezpłatne 16-kanałowe oprogramowanie.

Kamera będzie dostępna na przełomie listopada i grudnia.

*) Funkcja ta będzie dostępna w późniejszym terminie, poprzez aktualizację firmware'u.

Bezpośr. inf. Suma

Firma ADT walczy z rosnącym problemem kopiowania kart płatniczych

Firma ADT, lider rynku elektronicznych systemów zabezpieczeń oraz systemów ochrony, zaprezentowała rozwiązania służące do ochrony przed fałszerstwami kart kredytowych i debetowych polegającymi na kopiowaniu danych z paska magnetycznego.

Kopiowanie danych z kart w bankomatach (ATM) to rosnący problem międzynarodowy. Dane przedstawione przez reprezentanta europejskiej sieci bankomatów, European ATM Security Team (zespół do spraw bezpieczeństwa ATM), wykazują, że w roku 2006 w Europie zanotowano wzrost liczby incydentów związanych z kopiowaniem kart o 32% w porównaniu z rokiem 2005. Straty sieci ATM w roku 2006 przekroczyły 306 milionów euro, przy czym za zdecydowaną większość tych strat odpowiedzialny jest proceder kopiowania danych zawartych na kartach płatniczych.

Firma ADT zawarła sojusz strategiczny z firmą TMD Security, wiodącym dostawcą technologii zapobiegających kopiowaniu danych oraz producentem rozwiązania o nazwie Card Protection Kit + (CPK+). Zestaw produktów CPK+ oferowanych teraz przez firmę ADT umożliwia zabezpieczenie zarówno osób korzystających z bankomatów (ATM) i terminali samoobsługowych (SST), używanych np. do sprzedaży biletów kolejowych, jak i firm świadczących takie usługi swoim klientom.

Rozwiązania CPK+ pozwalają zabezpieczyć terminale ATM i SST zarówno przed mechanicznymi, jak i niemechanicznymi skanerami kart. Dostępny jest szeroki wybór opcji, pozwalający na zabezpieczenie się przed wszelkimi sposobami kopiowania danych, w tym między innymi przed urządzeniami umieszczanymi nad szczeliną na kartę, fałszywymi frontami bankomatów oraz urządzeniami montowanymi nad wejściem do pomieszczenia, w którym znajduje się terminal ATM lub SST. We wszystkich przypadkach zastosowana technologia, emitująca sygnał zakłócający pracę urządzenia skanującego, uniemożliwia przechwycenie danych z karty.

Rozwiązanie takie zapewnia szereg wyjątkowych korzyści. Blokując działanie urządzeń przechwytujących dane z karty, jednocześnie umożliwia normalne działanie terminala ATM lub SST, co oznacza brak przerw w obsłudze klientów i brak konieczności interwencji właściciela terminala. Dzięki temu można skrócić czas przestoju terminali i zmniejszyć koszty ich obsługi. Co więcej, w przypadku wykrycia próby fałszerstwa CPK+ może przesłać cichy alarm do właściciela terminala ATM lub SST. Oferowane produkty są proste w montażu, nie wymagają konfiguracji ustawień programowych w celu dostosowania ich do współpracy z konkretnymi terminalami, są niewidoczne na zewnątrz.

– *Kradzież pieniędzy z bankomatów to ulubione przez przestępców zastosowanie techniki kopiowania danych z kart. W Europie znajduje się ponad 330000 bankomatów* – powiedział Ken Scotland, wiceprezes działu Commercial Sales firmy ADT, działającego w Europie, na Bliskim Wschodzie i w Afryce. – *Te nowe produkty w połączeniu z naszym doświadczeniem w sektorze finansów i bankowości pozwolą rozwiązać ten problem i zapewnić ochronę zarówno klientom, jak i dostawcom usług.*

Rodzina produktów CPK+ jest stopniowo wprowadzana na rynki europejskie. Zostały już one wdrożone w Wielkiej Brytanii, w dobrze znanych grupach banków.

Bezpośr. inf. ADT Poland

Nowa rodzina kamer megapikselowych firmy Bosch

Firma **Bosch** przedstawia nową gamę rozwiązań z zakresu dozoru wizyjnego, oferujących obraz najwyższej rozdzielczości oraz niezwykłą elastyczność systemu. Kamery megapikselowe Bosch, dzięki przetwornikowi składającemu się z maks. 3,1 miliona pikseli, zapewniają niebywale ostry obraz o wysokiej jakości, zawierający detale, których nie dostrzegą inne kamery. Jedna kamera megapikselowa Bosch może objąć obszar tej samej wielkości, co sześć standardowych kamer analogowych. Dzięki temu możliwe jest zmniejszenie kosztów urządzeń i instalacji oraz serwisowania systemu.

Nowa rodzina kamer megapikselowych Bosch składa się z trzech modeli. Model podstawowy NWC-0700 wystarcza do uzyskania szczegółowego obrazu kolorowego dzięki przetwornikowi o rozdzielczości 2 Mpx.

Model kolorowy NWC-0800, wyposażony w przetwornik o rozdzielczości 3,1 Mpx, zapewnia bardziej szczegółowy obraz, umożliwiając uchwycenie mniejszych detali przy większej odległości obserwacji. Obraz z takiej kamery ma prawie siedem razy więcej pikseli w porównaniu do konwencjonalnych systemów CCTV o wysokiej rozdzielczości. W celu zapewnienia ciągłego, 24-godzinnego dozoru, dualny system NWC-0900 z dwoma przetwornikami składa się z 3,1-megapikselowej kamery kolorowej do użytku dziennego oraz 1,3-megapikselowej kamery monochromatycznej, przeznaczonej do pracy przy złym oświetleniu.

Przełączanie kamer odbywa się automatycznie, w zależności od poziomu oświetlenia. Wszystkie kamery są wyposażone w cyfrowe funkcje obrotu, pochylenia oraz zoomu, które umożliwiają użytkownikowi sprawdzenie z bliska szczegółów w dowolnym obszarze obrazu.

Kamery megapikselowe Bosch mogą być zastosowane w instalacjach cyfrowych, a także hybrydowych, we współpracy z cyfrowymi rejestratorami DiBos firmy Bosch. Jest to unikatowy i uniwersalny sposób rozszerzenia możliwości lub rozbudowy istniejących systemów analogowych. Nowe kamery dostarczają dodatkowych szczegółów tam, gdzie jest to potrzebne, zwiększając funkcjonalność konwencjonalnego dozoru wizyjnego w czasie rzeczywistym, szczególnie w obszarach podwyższonego ryzyka lub przy złym oświetleniu.

Przepustowość oraz wykorzystanie przestrzeni na dysku twardym mogą być optymalizowane dzięki regulowanej rozdzielczości oraz częstotliwości odświeżania. Dodatkowo kamery megapikselowe obsługują standard PoE (*Power over Ethernet* – zasilanie przez sieć Ethernet), co upraszcza instalację poprzez wyeliminowanie lokalnego źródła zasilania.

Kamery megapikselowe Bosch doskonale nadają się do dozoru wizyjnego rozległych obszarów, takich jak stadiony, budynki użyteczności publicznej, centra miast, oraz do obserwacji imprez masowych.

Bezpośr. inf. Robert Bosch Security Systems

Ostatnia w tym roku konferencja Sekcji MUZ

W dniu 21 września 2007 r. odbyła się kolejna konferencja z cyklu poświęconego wytwórstwu i dystrybucji Mechanicznych Urządzeń Zamykających (MUZ) na przykładzie firmy Gerda, zamykająca ten cykl w bieżącym roku.

W spotkaniu udział wzięli członkowie Sekcji MUZ i zaproszeni goście, w tym prowadzący prelekcję przedstawiciele Gerdy: Marek Głowicki i Jacek Kraśniewski.

Podczas spotkania omówiona została rola MUZ w zwiększaniu bezpieczeństwa osób i mienia. Prezes Sekcji MUZ odczytał projekt planu pracy Sekcji w roku 2008, który został jednogłośnie przyjęty przez obecnych członków. Przypomniał też członkom o potrzebie zgłaszania uwag do raportu o stanie branży MUZ w kraju. Raport ten Sekcja MUZ ma przedstawić komisji SIMP ds. współpracy z sekcjami i towarzystwami SIMP do końca 2008 r.

Przedstawiciele Gerdy przedstawili szczegółowo ofertę swoich produktów przeznaczonych do sprzedaży w kraju i kierowanych na eksport. Firma produkuje drzwi o zwiększonej odporności na włamanie wg wymagań przedmiotowej normy PN-90/B-92270, drzwi wzmocnione klasy 2. oraz drzwi klasy 3. i 4. wg wymagań normy PN ENV 1627, a także szereg zamków bezpośredniego ryglowania, wkładek kluczowych, kłódek oraz elementy wyposażenia (okucia budowlane), np. tarcze drzwiowe, klamki i samozamykacze, posiadające certyfikaty Zakładu Certyfikacji MUZ przy Instytucie Mechaniki Precyzyjnej (IMP). Na konferencji zaprezentowano szereg nowości mających na celu podwyższenie poziomu bezpieczeństwa osób i mienia. W bieżącym roku uzupełniono ofertę o drzwi zewnętrzne do domków jednorodzinnych o zwiększonej izolacyjności cieplnej i odporności na czynniki atmosferyczne. Firma oferuje instytucjom i zakładom wykonawstwo układów centralnego otwierania w systemach centralnego i grupowego klucza, centralnej wkładki i w systemie mieszanym.

Podczas spotkania przyjęto regulamin członków wspierających SIMP (przedstawiciele Gerdy rozważają możliwość zostania członkiem wspierającym Sekcji MUZ SIMP).

Była to ostatnia zorganizowana przez Sekcję MUZ konferencja w tym roku. W październiku, w Warszawskim Domu Technika NOT, odbyło się także szkolenie doskonalenia zawodowego w zakresie zamknięć, zorganizowane przez Sekcję we współpracy z Zakładem Doskonalenia Kadr SIMP.

mgr inż. mech. Józef Rudziński
prezes Sekcji MUZ SIMP

Panasonic CCTV Roadshow 2007

W dniu 9 października w siedzibie firmy **Panasonic Polska** odbyła się pierwsza z cyklu czterech prezentacji w ramach Roadshow 2007 systemów telewizji dozorowej. Na październikowe spotkania, zorganizowane w czterech miastach na terenie kraju (9.10. w Warszawie, 11.10. w Poznaniu, 16.10. w Krakowie, 18.10. we Wrocławiu), zaproszono przedstawicieli wszystkich zainteresowanych firm oraz instytucji, a także prasy branżowej – czasopism *Systemy Alarmowe* i *Zabezpieczenia*.

Szkolenie cieszyło się dużym zainteresowaniem, a wszystkie przygotowane przez organizatorów miejsca były zajęte.

Firmę Panasonic reprezentowali Trevor Brown (*Head of System Solutions CEE*), Hideo Hiraishi (*PSS Security Marketing Team*) oraz Dariusz Łabędzki (*Area Sales Manager*).

Dariusz Łabędzki przywitał wszystkich zebranych gości, a następnie, w kilku zdaniach, przedstawił historię firmy. Słuchacze mieli okazję dowiedzieć się, że Panasonic to marka handlowa koncernu Matsushita Electric Industrial, który jest jednym z największych na świecie producentów sprzętu elektronicznego i czołowym dostawcą produktów elektroniki użytkowej.

Przedsiębiorstwo założył Konosuke Matsushita w 1918 roku w Osace w Japonii; z trzech pracowników rozrosło się do 260000 zatrudnionych na całym świecie. Panasonic Polska funkcjonuje jako przedstawicielstwo handlowe koncernu od maja 1993 roku.

– *Panasonic jest jednym z czołowych producentów systemów telewizji dozorowej (w tym roku mija 50 lat od momentu pojawienia się pierwszej kamery* – powiedział Dariusz Łabędzki. – *Panasonic jest również pionierem we wprowadzaniu nowatorskich rozwiązań technologicznych, podnoszących jakość i zwiększających funkcjonalność systemów CCTV, a systemy zabezpieczeń ze znakiem Panasonic to gwarancja najwyższej jakości, niezawodności oraz bezpieczeństwa.*

Firma posiada w swojej ofercie cała gamę produktów (kamery, krosownice, rejestratory, monitory, urządzenia IP, oprogramowanie zarządzające itp.).

– *Panasonic preferuje sprzedaż kompletnych, bardzo efektywnych i niezawodnych systemów monitoringu wizyjnego, które działają o wiele lepiej niż systemy uzupełniane produktami innych producentów* – powiedział Dariusz Łabędzki.

Prezentacja była prowadzona bardzo sprawnie i ciekawie. W pierwszej części obejmowała systemy analogowe, w drugiej organizatorzy przedstawili sieciowe rozwiązania telewizji dozorowej. Szczególne zainteresowanie oraz pytania uczestników dotyczyły produktów IP, wśród których firma Panasonic posiada wiele innowacyjnych rozwiązań.

Dużo uwagi prowadzący poświęcili autonomicznym rejestratorom sieciowym serii I-PRO WJ-ND200 i WJ-ND300A. Urządzenia te pozwalają na rejestrację strumieni wideo z 16 lub nawet 32 kamer. Co najważniejsze, urządzenia te, w porównaniu do systemów rejestracji opartych na komputerach PC z systemem operacyjnym Windows, gwarantują wyższy poziom bezpieczeństwa. Wątek bezpieczeństwa oraz profesjonalizacji systemów CCTV często przewijał się podczas szkolenia.

Efektowna multimedialna formuła prezentacji (poszczególne cechy produktów ilustrowane były krótkimi filmami, pozwalającymi uczestnikom docenić zalety przedstawionych rozwiązań) sprawiła, iż konferencja jeszcze bardziej zyskała na atrakcyjności.

W trakcie przerwy oraz po szkoleniu, podczas rozmowy z osobami prowadzącymi, istniała możliwość praktycznego zapoznania się z produktami firmy Panasonic oraz ewentualnego uzupełnienia wiedzy.

Teresa Karczmarzyk
Patryk Gańko

Pokaz premierowy Integral Evolution

Nowości z firmy **Schrack Seconet** – centrala systemu sygnalizacji pożarowej Integral Evolution wraz z nową, wielosensorową czujką **Cubus MTD 533** – zostały zapowiedziane na III kwartał br. już w czerwcu, podczas Ogólnopolskiego Szkolenia Projektowego'2007. 26 września 2007 roku odbył się w Warszawie **pokaz premierowy** tego systemu, połączony z konferencją prasową.

Pokaz zaszczycił swoją obecnością ambasador Austrii – **dr Alfred Längle.** W wydarzeniu tym uczestniczyło łącznie ok. 60 gości, reprezentujących głównie partnerów Schrack Seconet Polska. Przybyło 14 przedstawicieli dziesięciu wydawnictw branżowych. Obecna była także liczna grupa pracowników firmy Schrack Seconet Polska z prezesem zarządu **Grzegorzem Ćwiekiem** na czele oraz przedstawiciel siedziby głównej (Schrack Seconet AG Austria) – **Herbert Hübl.**

Nove Kino PRAHA, gdzie odbył się pokaz, umożliwiło pokazanie na dużym ekranie filmu prezentującego system Integral Evolution. Można było także obejrzeć z bliska zarówno samą centralę, jak i nowa czujkę. Przed filmem prezes Ćwiek przywitał zgromadzonych gości, po czym oddał głos ambasadorowi Längle, który w języku polskim przypomniał historię firmy Schrack Seconet oraz przedstawił w skrócie jej obecne dokonania.

– *Firma Schrack jest wspaniałym przykładem pełnej sukcesów działalności austriackich firm w Polsce. Jest obecna zarówno w wymianie handlowej oraz inwestycjach. Wymiana handlowa wyniosła w roku ubiegłym 4 mld euro. Łącznie austriackie inwestycje w Polsce od roku 1989 do dzisiaj wynoszą ok. 3 mld euro. Firma ma przedsiębiorstwa – córki w Polsce, Szwecji i na Węgrzech oraz przedstawicielstwa w Słowacji i w Rosji* – powiedział Längle.

Początki przedsiębiorstwa przypadają na okres wielkiej rewolucji przemysłowej XIX wieku, kiedy to na terenie dzisiejszej Austrii i Niemiec powstawały pierwsze zakłady produkujące urządzenia elektrotechniczne, stanowiące podwaliny dzisiejszych koncernów nie tylko w Europie, ale i w Stanach Zjednoczonych oraz Japonii. Pierwowzorem obecnych systemów sygnalizacji pożarowej były urządzenia produkowane przez Radiolaboratorium doktora Eduarda Schracka już w pierwszych latach XX wieku. Po przerwie wywołanej zniszczeniami II wojny światowej produkcja ta jest kontynuowana do dnia dzisiejszego [1].

Oczywiście jest to już produkcja innych urządzeń. W latach siedemdziesiątych ubiegłego stulecia w firmie Schrack powstała jedna z pierwszych na świecie sterowana mikroprocesorowo centrala sygnalizacji pożarowej. Produkt ten przez lata ulegał ewolucji, aby dziś, pod nazwą Integral Evolution, mógł poszczycić się także zmianami, które można nazwać rewolucyjnymi. Mówił o nich prezes Ćwiek już po zakończeniu prezentacji filmowej. Jedną z nich jest wprowadzenie do systemu zupełnie nowej czujki Cubus MTD 533, która zastąpi dotychczas stosowane w systemie elementy detekcyjne. Spełnia ona wymagania całego zakresu testów dotyczących różnych typów pożaru (od TF1 do TF9) i w związku z tym może być wykorzystana w każdych zastosowaniach z zakresu SSP. Firma Schrack Seconet uzyskała na nią odpowiednie certyfikaty europejskie. Czujka przeszła także pozytywnie badania w CNBOP.

Schrack Seconet Polska powstała w 1998 roku, stając się od tej pory jedynym bezpośrednim reprezentantem producenta w naszym kraju. O ciekawych aspektach kontaktów firmy Schrack Seconet z profesjonalistami z Polski opowiedział, już po prezentacji filmu, jej przedstawiciel z Wiednia – Herbert Hübl. Inżynierowie firmy Schrack Seconet wnieśli wielki wkład w rozwój systemów bezpieczeństwa także dzięki pracy profesjonalistów z naszego kraju, którzy okazali się bardzo kompetentnymi partnerami. Obecnie pierwszym krajem eksportowym dla Schrack Seconet są Niemcy, a spośród pozostałych 20 partnerów handlowych Polska generuje 15% eksportu, zajmując zaszczytną drugą pozycję. Dotychczas sprzedano w Polsce ok. 1350 systemów sygnalizacji tej firmy.

Kolejną częścią spotkania, po wystąpieniu Herberta Hübla, były pytania i odpowiedzi, których udzielali dyrektor techniczny Schrack Seconet Polska **Krzysztof Kunecki** oraz prezes Grzegorz Ćwiek, który na wstępie wyjaśnił, jakie są istotne różnice pomiędzy dotychczas oferowanym modelem centrali Integral a wyglądającą z zewnątrz bardzo podobnie jej nową wersją – Integral Evolution.

Sama obudowa uległa niewielkim zmianom – jest teraz bardziej obła – ale wewnątrz niej znajdują się obecnie nowe karty, w tym karta z procesorem AMD, zapewniającym 400 razy szybszą pracę systemu niż dotychczas stosowany procesor. O 40% bardziej wydajny jest nowy zasilacz, co przekłada się na obniżenie kosztów budowy systemu, gdyż można teraz podłączyć do niego większą liczbę urządzeń. **Bufor zdarzeń,** gromadzony na dołączanej dodatkowo karcie pamięci SD, pomieści ich aż 65000, przez co centrala Integral Evolution spełnia ostatnio wprowadzone w życie wymagania w tym zakresie (od sierpnia br., zgodnie z rozporządzeniem MSWiA z czerwca br., minimalna pojemność powinna wynosić 9999 zdarzeń) i staje się bezkonkurencyjna wśród innych produktów tego typu na rynku. W samej centrali można wykorzystać łącznie do 160 wyjść przekaźnikowych, nie licząc tych, które są podłączane na pętlach.

Nowe rozwiązania tworzone są w Schrack Seconet przez kolejne pokolenia inżynierów. Wiele z nich powstało z inicjatywy polskich specjalistów i było odpowiedzią na wysokie wymagania, formułowane przez inwestorów budujących nowe obiekty w Polsce (pod tym względem rynek polski należy do najbardziej wymagających na świecie). Dzięki ciągłości myśli technicznej bez trudu zapewniono kompatybilność wstecz, co nie jest powszechne wśród tego

typu systemów. Nawet niektóre elementy systemu sprzed 30 lat są w stanie nadal współpracować z nowymi centralami (na lotnisku Schwechat pod Wiedniem działa system składający się m.in. z ok. 50 central czterech różnych generacji). Nowy zasilacz może być z powodzeniem stosowany w systemach z centralami BMZ Integral. Duża elastyczność systemu, podwójna redundancja (sprzętowa i programowa) i inne cechy systemu Integral Evolution sprawiają, że, według słów prezesa Ćwieka, nie ma obecnie algorytmów, które nie mogłyby zostać w nim zrealizowane.

W dyskusji, jaka wywiązała się podczas sesji pytań i odpowiedzi, wzięli udział specjaliści w dziedzinie SSP.

Pierwsze z pytań dotyczyło zakresu wprowadzonych w Integral Evolution zmian, w tym odnoszących się do transmisji sygnałów. Prezes Ćwiek wyjaśnił, że chociaż najistotniejsze zmiany dotyczą oprogramowania systemu, to, zgodnie z filozofią firmy Schrack Seconet, nakazującą aby do doskonałości dochodzić w sposób ewolucyjny, dzisiejsze zmiany nie sprawią żadnych kłopotów osobom programującym nowy model centrali, a sam protokół komunikacyjny pozostaje na razie w takim samym stadium. Serwisanci i programiści systemu już od sześciu miesięcy znają nowe funkcje serwisowe i użytkowe. W przypadku Integral Evolution można mówić o kompatybilności nie tylko wstecz ale i w przód, gdyż nowe oprogramowanie jest dostosowane także do funkcji dopiero planowanych.

Wieloletni były prezes zarządu Schrack Seconet **Piotr Pajor** spytał o możliwości i ograniczenia nowego systemu – ile obiektów można nim nadzorować, ile czujek podłączyć i czy istnieją takie wymagania w projektach realizowanych w kraju i za granicą, że Schrack Seconet nie może ich spełnić. Odpowiedź na te pytania zawiera się w jednym stwierdzeniu Grzegorza Ćwieka: „Nie ma praktycznie żadnych ograniczeń". W jednym rozległym systemie można podłączyć do sześćdziesięciu kilku tysięcy central, ale jest to ograniczenie teoretyczne. Liczba central w największych obiektach umieszczonych na liście referencyjnej Schrack Seconet to kilkadziesiąt, a nawet ponad sto, ale to nadal liczby bardzo odległe od granic teoretycznych. Poza nielicznymi wyjątkami nie powstają na ogół ani w Europie Zachodniej, ani w Azji tak skomplikowane obiekty jak w Polsce. Polscy specjaliści zgłaszali wymagania, które w innych krajach nie występowały, wnosząc w ten sposób wkład w rozwój systemów. Mają w tym udział zarówno polscy eksperci, jak i strażacy.

Odpowiedź na kolejne pytanie – czy Integral Evolution ma dopuszczenie do sterowania urządzeniami gaszenia – brzmiała: „Tak, to jedyny system umożliwiający integrację z SUG; należy w tym celu umieścić w centrali specjalną kartę i ewentualnie panel informacyjny, co jest rozwiązaniem znacznie tańszym niż instalacja odrębnego systemu".

Następne pytanie związane było z wizualizacją stanu i pracy rozbudowanych systemów, gdy panel obsługi w centrali nie jest wystarczający. W takich przypadkach stosowana jest nowa wersja systemu komputerowego o nazwie Secolog, obsługującego jeden albo dwa duże, kolorowe wyświetlacze LCD.

Zdaniem Herberta Hübla z siedziby głównej Schrack Seconet, który także zabrał głos w dyskusji, Polska ma jedne z najlepszych standardów przeciwpożarowych na świecie. Właściwe zabezpieczenie wymaga jednak niezawodnych rozwiązań, choć nie są one najtańsze. Ważne jest, aby pieniądz nie rządził i nie decydował o rozwiązaniach technicznych, aby poziom instalacji SSP był utrzymywany na najwyższym możliwym poziomie. W przeszłości systemy Schrack Seconet nie były konkurencyjne cenowo. Dzięki temu, że firma od lat nie podnosi cen swoich wyrobów, a dwa lata temu dokonała obniżki cen central o 40%, co było możliwe dzięki istotnemu wzrostowi sprzedaży w Polsce (obecnie poprzez sieć ok. 30 autoryzowanych partnerów), dziś ceny są porównywalne także z produktami krajowymi.

Ostatnie z pytań dotyczyło sposobów integracji Integral Evolution z systemami zarządzającymi typu BMS (*Building Management Systems*). Taka integracja jest możliwa nie tylko z produktami takich firm, jak Honeywell, Johnson Control czy Siemens, ale praktycznie z dowolnymi innymi. Wprawdzie firma Schrack Seconet nie rozpowszechnia z zasady swojego protokołu komunikacji, ale może udostępnić fachowcom gotowe, już wypracowane procedury integracyjne, a nawet, gdy istnieje taka potrzeba, także sam protokół. Dzięki temu, że partnerzy Schrack Seconet mają już opracowane i sprawdzone rozwiązania integracyjne, wykorzystujące platformę BACnet oraz serwer OPC, wystarczy zgłosić się do firmy i ustalić warunki przekazania tych rozwiązań, zamiast tworzyć od podstaw własne rozwiązania.

Po części informacyjnej przybyli goście mieli okazję spróbować specjałów kuchni egzotycznej w restauracji Babalu, mieszczącej się nieopodal miejsca, w którym zorganizowano pokaz.

Adam Bułaciński

[1] Materiały z pokazu premierowego Integral Evolution

Sprawozdanie z seminarium technicznego WAT pt. „Trendy rozwojowe technicznych systemów bezpieczeństwa”

W dniach 27 i 28 września 2007 roku odbyło się na terenie Wojskowej Akademii Technicznej w Warszawie seminarium techniczne pt. „Trendy rozwojowe technicznych systemów bezpieczeństwa”, zorganizowane przez Instytut Inżynierii Systemów Bezpieczeństwa, **Instytut Systemów Elektronicznych Wydziału Elektroniki WAT** oraz **Instytut Optoelektroniki WAT.** Sponsorami seminarium były firmy GE Security Polska, Bosch Security Systems (integralny dział firmy Robert Bosch) oraz CardCo, a sponsorem medialnym – czasopismo *Zabezpieczenia*.

W seminarium wzięło udział ok. 70 osób, głównie absolwentów studiów podyplomowych „Techniczna ochrona osób i mienia”, pracowników WAT i innych osób związanych zawodowo z tematyką zaawansowanych systemów bezpieczeństwa. Z uwagi na to, że w tym roku zakończyła się jubileuszowa, dziesiąta edycja studiów podyplomowych, prowadzonych na Wydziale Elektroniki WAT, seminarium połączono ze zjazdem koleżeńskim ich absolwentów.

Wprowadzenia do seminarium dokonał **dr hab. inż. Tadeusz Dąbrowski,** profesor WAT i dyrektor Instytutu Systemów Elektronicznych Wydziału Elektroniki WAT. Przedstawił on m.in. historię podyplomowych studiów z zakresu ochrony osób i mienia, zainicjowanych i prowadzonych przez pierwsze sześć edycji przez **dr hab. inż. Czesława Przybysza,** profesora nadzwyczajnego WAT (w tym czasie pod nieco inną nazwą: „Fizyczna i techniczna ochrona osób i mienia”). Kierownikiem studiów przez kolejne dwie edycje był **dr inż. Krzysztof Serafin,** następnie ponownie prof. Przybysz, a ostatnio – **dr inż. Krzysztof Kwiatos.** Najliczniejszą grupę absolwentów studiów, spośród 179 osób, które je dotychczas ukończyło, stanowią pracownicy banków, a następnie wojska i straży granicznej.

Prof. Dąbrowski podał także krótką informację o Instytucie Systemów Elektronicznych, na terenie którego odbyło się seminarium, w tym o jego strukturze, prowadzonych przedmiotach i specjalnościach oraz o kierunkach działalności naukowo-badawczej Instytutu.

Następnie przybyłych gości, a także przedstawicieli sponsorów i patrona medialnego, powitał w imieniu organizatorów **mgr inż. Ireneusz Krysowaty,** po czym rozpoczęła się część merytoryczna. W ciągu dwóch dni miało miejsce w sumie 13 wystąpień – referatów, prezentacji i wykładów.

1. „Trendy w optoelektronicznych systemach ochrony perymetrycznej” – prof. dr hab. inż. Mieczysław Szustakowski (WAT)

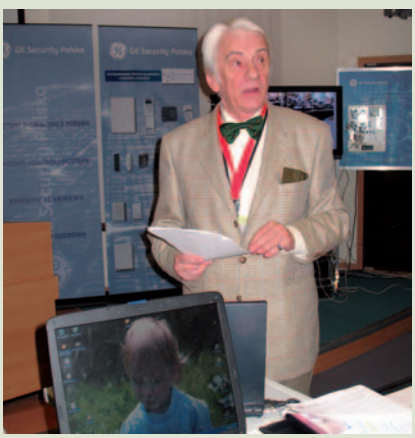
Autorami tego referatu byli także współpracownicy prof. Szustakowskiego, a wśród nich wieloletni pracownik WAT – **dr inż. Wiesław M. Ciurapiński.** Pierwsza część referatu dotyczyła rozwoju technologii detekcji światłowodowej, kolejna – dozoru wizyjnego i radarowego, a ostatnia – trendów w dziedzinie inteligentnych rozwiązań sieciowych i teleinformacyjnych systemów łączności.

Współczesne światłowodowe systemy ogrodzeniowe mogą chronić obszary o obwodzie kilkudziesięciu kilometrów z dokładnością lokalizacji intruza rzędu 25 m. Warto podkreślić, że także WAT posiada swoje rozwiązanie czujnika światłowodowego i poszukuje firmy do współpracy w zakresie tego typu interferometrycznej detekcji światłowodowej. W dziedzinie wideodetekcji coraz bardziej powszechne stają się kamery termowizyjne oraz nowe rozwiązania, które do wykrywania intruza wykorzystują radary. Wyraźna jest tendencja do ograniczania liczby rejestrowanych i prezentowanych obrazów tylko do tych, które są naprawdę użyteczne. Interesującym rozwiązaniem w tym zakresie jest technologia *Image Fusion*, pozwalająca na automatyczną obróbkę sygnału z dwóch kamer w celu uzyskania jednego obrazu i automatycznej detekcji zagrożenia. Dzięki inteligentnym systemom dozoru wizyjnego IVS (*Intelligent Video Surveillance*) można nie tylko zrealizować rozmaite algorytmy detekcji intruza, ale także np. automatycznie wykrywać bagaż pozostawiony bez dozoru. W nowoczesnych perymetrycznych systemach bezpieczeństwa dużą rolę odgrywają technologie sieciowe, umożliwiające połączenie inteligentnych kamer sieciowych INC (*Intelligent Network Camera*), będących źródłami cyfrowego i skompresowanego sygnału wizyjnego, z serwerami, na których następuje automatyczna obróbka obrazu, a także ze stacjami roboczymi.

2. „Systemy zabezpieczeń wykorzystujące podczerwień i technikę laserową” – prof. dr hab. inż. Zbigniew Bielecki (WAT)

W referacie zostały omówione następujące zagadnienia:

- tendencje w zakresie układów detekcji promieniowania optycznego (technologie MOCVD, MBE, zaawansowane procesory krzemowe, mikromechanika krzemowa);
- aktywne i pasywne systemy ochrony obiektów, w tym wykorzystujące podczerwień i czujniki światłowodowe;
- systemy wykrywania oraz identyfikacji gazów i bakterii z próbkowaniem w miejscu występowania skażenia oraz systemy zdalnego monitoringu, niewymagające w zasadzie kontaktu z obszarem skażenia;
- optoelektroniczne systemy monitoringu zanieczyszczeń środowiska – aktywne, o zasięgu 10–50 m i czułości 10 ppm, oraz pasywne, o zasięgu ponad 100 m i czułości 500 ppm – m.in. laserowy system DIAL (*Differential Absorption Lidar*) do zdalnej detekcji metanu;
- systemy rozpoznania wielospektralnego, znajdujące zastosowanie m.in. w ochronie antyrakietowej (zintegrowany system



optoelektroniczny obejmuje systemy ostrzegania, śledzenia celu oraz oślepiający).

Odnośnie systemów zdalnego monitoringu należy wyjaśnić, że mogą to być systemy typu *stand-off*, umożliwiające wykrywanie chmur gazów lub bakterii ze znacznej odległości, bez kontaktu ze skażeniem (metodami aktywnymi lub pasywnymi), oraz typu *remote*, w których wykorzystuje się niewielkie czujniki punktowe *in situ*, przy czym dane z tych czujników są przesyłane przewodowo lub bezprzewodowo do centrów alarmowych.

3. „Podstawowe zasady zapewniania bezpieczeństwa osób i mienia" – dr Zbigniew Nowicki

W swoim wykładzie gen. Nowicki omówił organizację komercyjnych działań ochronnych, zgodnych z obowiązującą ustawą o ochronie osób i mienia. Przed dokonaniem wyboru sposobów i środków ochrony należy postępować zgodnie z dwiema zasadami: po pierwsze należy sprecyzować rodzaje zagrożeń (pomocne są w tym m.in. zaprezentowane modele „trójkąta bezpieczeństwa" oraz „rozety zagrożeń"), po drugie – trzeba sobie uświadomić, że nie ma jednego „złotego" środka ochrony; wszystkie środki należy traktować jako elementy pewnego systemu, uwzględniając spodziewany czas reakcji na zagrożenie. Wzięte z życia obserwacje wskazują także na potrzebę dodania do wyżej wymienionych zasad także zasady fundamentalnej, zerowej: „Nie dajmy się zwariować". Należy stosować środki adekwatne do realnych zagrożeń. Nie można pozwolić sobą manipulować ani narzucać rozwiązań nieprzystających do potrzeb. Należy pamiętać o tym, że żadne zabezpieczenie nie daje stuprocentowej pewności. Trzeba brać pod uwagę również to, że źródłem zagrożenia dla osób i mienia może być nie tylko intruz, ale i pracownik własnej firmy albo kontrahent. Analizując możliwe środki neutralizacji zagrożeń, warto zapoznać się z modelem „kalejdoskopu bezpieczeństwa", w którym centralnym punktem jest BEZPIECZEŃSTWO.

4. „Metody podprogowego przesyłania informacji w sygnałach akustycznych" – dr hab. inż. Jerzy Łopatka (WAT)

W referacie zdefiniowano pojęcie transmisji podprogowej, czyli tzw. znaku wodnego, a następnie omówiono klasyfikację metod transmisji i wymagania stawiane systemom transmisji podprogowej oraz porównano różne metody takiej transmisji. Znak wodny (ang. *watermark*) to sygnał informacyjny, który jest celowo dodany do użytecznego sygnału – w tym przypadku akustycznego – w sposób niedostrzegalny dla słuchacza. Ma zastosowanie w ochronie praw autorskich, weryfikacji integralności podpisów, a także korespondentów, badaniach rynkowych i ukrywaniu informacji (w celu skrytego przesyłania danych). Powinien być odporny na celowe lub przewidywalne manipulacje (np. na dodanie szumu, filtrację), prowadzić do dużego zniekształcenia sygnału znakowanego w przypadku usunięcia lub zmiany znaku wodnego i umożliwiać kontrolę integralności i kompletności sygnału znakowanego.

Chociaż tematyka referatu nie należała do najłatwiejszych, to został on zaprezentowany w jasny i atrakcyjny sposób. Uczestnicy seminarium mieli okazję usłyszeć zarówno przykłady sygnałów wyjściowych, poddawanych następnie znakowaniu, próbki znaków wodnych, wykorzystujących różne metody kodowania, jak i efekty końcowe, nie różniące się dla słuchacza od sygnałów wyjściowych.

5. „Nowości w zabezpieczeniach mechanicznych i elektromechanicznych oraz architektoniczno-budowlanych" – dr inż. Robert Ćwirko (WAT)

O tym, że w dobie coraz bardziej zaawansowanych elektronicznych systemów służących do ochrony mienia zabezpieczenia mechaniczne nie tracą na znaczeniu świadczyć może fakt, że najważniejsze miejsca w bankach szwajcarskich, takie jak skarbce itp., są nadal zabezpieczane głównie w sposób mechaniczny. W odróżnieniu od systemów elektronicznych, które reagują na zdarzenia, zabezpieczenia mechaniczne ograniczają ryzyko ich wystąpienia i dlatego są tam uważane za bardziej skuteczne.

Autor referatu przedstawił wpływ rozwiązań architektoniczno-budowlanych na poziom bezpieczeństwa obiektów specjalnych na podstawie ilustrowanej ciekawymi fotografiami i danymi analizy wydarzeń związanych z atakiem 11 września 2001 r. na Pentagon i budową ambasady amerykańskiej w Moskwie. Okazało się, że liczba ofiar ataku na Pentagon była znacznie mniejsza niż oczekiwali terroryści, gdyż zewnętrzne ściany budynku wzmocniono konstrukcjami stalowymi, zdolnymi udźwignąć grube, kuloodporne szyby, które zainstalowano w oknach zewnętrznych. Konstrukcje te uratowały także budynek przed zawaleniem się.

Autor zaprezentował także różnego rodzaju szyfrowe zamki mechaniczno-elektryczne, m.in. zamki odporne na podsłuch i prześwietlanie (stosowane w celu ustalenia położenia wycięć decydujących o otwarciu zamka, czemu zapobiega się w prezentowanym rozwiązaniu dzięki zastosowaniu w zamku elementów plastikowych), zamki do bankomatów z tzw. oknem czasowym oraz zamki sieciowe IP.

6. „Bezpieczeństwo informacji – teoria i praktyka problemu" – dr inż. Marek Blim i mgr inż. Paweł Niedziejko (WAT)

Punktem wyjścia powyższego referatu, wygłoszonego przez dr Blima, jest stwierdzenie, że „bezpieczeństwo nie jest stanem trwałym", które jest szczególnie trafne w przypadku, gdy mowa o bezpieczeństwie informacji. Ochrona informacji wymaga uświadomienia sobie zarówno jej wagi i wartości, jak i zagrożeń oraz rodzajów ryzyka, jakie mogą towarzyszyć takiej działalności.

W referacie omówiono problematykę ochrony informacji, począwszy od zwrócenia uwagi na konieczność konsekwentnego wdrażania w firmie, organizacji, grupie społecznej itp. podstawowych zasad i minimalnych wymagań dotyczących bezpieczeństwa informacji. Zwrócono uwagę na przejście od podstawowych działań organizacyjnych do operacyjnego zapewnienia bezpieczeństwa. Przypomniano kilka „oczywistych" prawd (informacja jest aktywem, bezpieczeństwo jest podstawą biznesu, bezpieczeństwo informacji jest w biznesie koniecznością, a plan bezpieczeństwa informacji jest budowany z uwzględnieniem określonych warunków, występujących w samej organizacji). Omówiono pięć faz poprawnej budowy planu bezpieczeństwa (inspekcja, ochrona, wykrywanie, reakcja

i refleksja) i przedstawiono współzależność polityk bezpieczeństwa operacyjnego firmy (współzależność polityki bezpieczeństwa personalnego, fizycznego, informacji oraz polityki ciągłości działania). Wspomniano także o normach regulujących zagadnienia, związane z bezpieczeństwem informacji (np. PN-ISO/IEC 27001:2007) oraz o standardzie zarządzania ryzykiem, firmowanym przez *Federation of European Risk Management Associations* (FERMA).

7. Prezentacja firmy GE Security Polska oraz jej oferty – Kazimierz Kacprzyk i Maciej Brzyski (GE Security Polska)

GE jest międzynarodową korporacją, działającą w branży technologicznej, usługowej oraz finansowej. Została założona przez Thomasa Edisona w roku 1878 jako Edison Electric Co. GE Security jest jedną z firm działu GE Industrial z siedzibą główną w Stanach Zjednoczonych. Warto podkreślić, że w Polsce mieści się jedno z sześciu centrów wdrożeniowych (R&D) GE Security.

O historii, strukturze i zakresach działalności GE mówił Kazimierz Kacprzyk, natomiast Maciej Brzyski zaprezentował zintegrowany system bezpieczeństwa Advisor Master, w którym system sygnalizacji włamania i napadu jest zintegrowany z kontrolą dostępu oraz nadzorem wizyjnym. W tym systemie zdarzenia są zapisywane wraz z towarzyszącym im obrazem. Istnieje możliwość wyszukiwania według słów kluczowych. Omówiono także inteligentną telewizję dozorową, umożliwiającą np. wykrywanie osób wchodzących do garaży podziemnych (bez reakcji na ruch pojazdów oraz osób przemieszczających się na zewnątrz garażu) i cyfrową analizę obrazu pod kątem występujących zagrożeń, takich jak np. podejrzane zachowanie ludzi.

8. „Kierunki rozwoju nowoczesnych systemów CCTV" – Józef Bycul (Bosch Security Systems)

Po zaprezentowaniu firmy Bosch, która, jak warto zaznaczyć, przeznacza większość swoich zysków na niekomercyjne działania Fundacji Boscha, jej przedstawiciel omówił rozwiązania wykorzystujące technologie sieciowe w systemach telewizji dozorowej. Takie rozwiązania, zawierające megapikselowe kamery IP, przełączniki sieciowe oraz routery, stały się w ciągu ostatnich trzech lat dominującym kierunkiem rozwoju telewizji dozorowej. Za transmisję sygnałów odpowiedzialna jest tu sieć Ethernet, a elementem, który archiwizuje, wizualizuje oraz integruje system telewizji dozorowej z innymi systemami jest oprogramowanie. Zgodnie z podejściem firmy Bosch za analizę obrazu odpowiadać powinien procesor kamery, co przy rozległych systemach pozwala na ograniczenie wymagań odnośnie przepływności serwerów, gdyż przesyłany jest obraz wynikowy. Tradycyjne podejście, o ile można w przypadku systemów CCTV IP mówić o jakiejkolwiek tradycji (pojęcie CCTV IP jest samo w sobie sprzeczne, gdyż otwartości związanej z sieciami IP towarzyszy określenie closed – przyp. autora tego sprawozdania), zakłada wykorzystywanie serwerów do przetwarzania obrazu, ale oznacza to, że docierają do nich także informacje zbędne, niepotrzebnie zajmując kanały transmisyjne.

Nowoczesna telewizja dozorowa, dzięki zaawansowanym algorytmom analizy obrazu, takim jak VCA (*Video Content Analysis*), umożliwia np. śledzenie obiektów (z zaznaczaniem ich trajektorii) podczas opadów śniegu i innego rodzaju trudnych warunków atmosferycznych, co zostało zaprezentowane na filmie. Uczestnicy seminarium mogli także przekonać się o skuteczności funkcji stabilizacji obrazu (*Video Stabilization Feature*), porównując ten sam obraz uzyskany bez wykorzystania tej funkcji i po jej zastosowaniu.

9. Blok dyskusyjny poświęcony współczesnym problemom bezpieczeństwa – prof. dr hab. inż. Mieczysław Szustakowski (WAT)

Pierwszy dzień seminarium zakończył blok dyskusyjny, na wstępie którego prof. Szustakowski omówił konferencję stowarzyszenia SPIE. Odbyła się ona we wrześniu br. we Florencji i składała się z sześciu sesji tematycznych, poświęconych m.in. rozwiązaniom służącym do monitorowania oceanu i wybrzeży, zdalnym sensorom elektrooptycznym, technologii optycznego przeciwdziałania (np. w celu oślepiania kamer) i nowym technologiom oraz materiałom dla celów obronnych. W dyskusji, jaka się następnie wywiązała, wzięło udział blisko dziesięciu uczestników seminarium.

Na zakończenie bloku dyskusyjnego prezes zarządu Instytutu Inżynierii Systemów Bezpieczeństwa – Paweł Niedziejko – wręczył prof. Szustakowskiemu dyplom uznania za wybitne zasługi w propagowaniu i budowaniu systemów bezpieczeństwa.

10. „Telemetryczny monitoring obiektów oddalonych z wykorzystaniem przewodowej i bezprzewodowej transmisji pakietowej" – dr inż. Krzysztof Serafin (NBP, Komitet Techniczny nr 52 d/s Systemów Alarmowych PKN)

Autor pierwszego referatu w drugim dniu seminarium omówił stosowane w systemach telemetrycznych protokoły przewodowej transmisji danych, pakietowe przesyłanie danych, wykorzystywane dzięki usłudze GPRS udostępnionej przez operatorów GSM, a także przykłady oprogramowania służącego do wizualizacji stanu monitorowanych obiektów. Zwrócił uwagę na praktyczne aspekty analizy gromadzonych danych o zdarzeniach występujących w takich obiektach.

11. „Systemy automatycznej identyfikacji – biometria, RFID" – mgr inż. Ireneusz Krysowaty i mgr inż. Przemysław Mierzwiak (WAT), „Urządzenia i systemy biometryczne" – Michał Koralewski (CardCo) – referaty połączone

Zapotrzebowanie na technologie weryfikujące tożsamość znacznie zwiększyło się w ciągu ostatnich kilku lat. O nowych rozwiązaniach w tej dziedzinie, niektórych jeszcze szerzej nieznanych (jak np. urządzenia rozpoznające szmer składanego podpisu, systemy identyfikacji na podstawie analizy gestów i chodu człowieka bądź ruchu jego oka albo ust), mówił Ireneusz Krysowaty. Z biometrią związane są także rozwiązania typowo militarne, np. mundury wojskowe z czujnikami funkcji życiowych.

Przemysław Mierzwiak omówił znaną i stosowaną od lat technologię identyfikacji radiowej (RFID), zwracając uwagę na postęp, jaki dokonał się w tej dziedzinie. Zwiększony, w porównaniu z pierwszymi konstrukcjami wykorzystującymi RFID, zasięg odczytu i zapisu, zadowalająca szybkość transmisji i duża odporność na zakłócenia

powodują, że pojawiają się całkiem nowe możliwości zastosowań tej technologii, nie tylko w kontroli dostępu (np. w przemyśle – do śledzenia procesu produkcji, w logistyce – do lepszej kontroli zapasów i stanu realizacji zamówień). Należy jednak mieć świadomość zagrożeń, jakie mogą być związane ze stosowaniem nowych technologii radiowych – także zdrowotnych (liczba komórek rakowych u badanych przez naukowców myszy wzrosła dwukrotnie po wszczepieniu urządzeń RFID).

Michał Koralewski pokazał z kolei zaawansowane czytniki biometryczne, przeznaczone do kontroli dostępu, w tym innowacyjny terminal biometryczny Biostation, zapewniający dużą szybkość i wysoki poziom identyfikacji linii papilarnych oraz zróżnicowany sposób interakcji multimedialnej z użytkownikiem. Innym ciekawym urządzeniem, które uczestnicy seminarium mogli obejrzeć w działaniu, był kontroler biometryczny VP-II do identyfikacji osób, wykorzystujący unikatowy algorytm rozpoznawania naczyń krwionośnych dłoni.

12. Warsztaty techniczne – Tomasz Żuk (GE Security Polska)

W ramach pierwszych warsztatów technicznych zaprezentowano m.in. zintegrowany system bezpieczeństwa Alliance 8300, stanowiący inteligentną platformę, w której system włamania i napadu łączy się z systemem kontroli dostępu, wykorzystującą jako medium transmisyjne sieci IP. Jest to system wielostanowiskowy, umożliwiający zarządzanie bezpieczeństwem w wielu lokalizacjach, które mogą być rozsiane po cały świecie. Omówiono także inne produkty z oferty firmy GE Security z zakresu telewizji dozorowej oraz systemów sygnalizacji pożaru.

13. Warsztaty techniczne – Józef Bycul i Arkadiusz Gmitrzak (Bosch Security Systems)

Również drugie warsztaty techniczne były poświęcone omówieniu produktów, tym razem oferowanych przez Bosch Security Systems urządzeń i systemów telewizji dozorowej. Zwrócono uwagę m.in. na to, że intensywnie rozwijające się systemy z kamerami megapikselowymi, które transmitują obraz przez sieci IP, wymagają odpowiednich przepływności sieci, a także dużych szybkości pracy CPU i kart graficznych komputerów. Mimo zalet, jakie daje możliwość wykorzystania w tym celu, bez dodatkowych nakładów, istniejących w firmach sieci komputerowych, zaleca się stosowanie wydzielonych sieci. Jedynie sieci „gigabajtowe" pozwalają niekiedy na wspólne wykorzystywanie zasobów sieciowych do różnych celów, a i w takim przypadku należy być świadomym, jakie są wymagania dotyczące przepływności, wynikające ze stosowania kamer megapikselowych.

Na zakończenie seminarium głos zabrali Tadeusz Dąbrowski i Paweł Niedziejko, po czym nastąpiło rozdanie certyfikatów jego uczestnikom.

W podsumowaniu warto zauważyć, że dzięki takim seminariom uczestnicy mogą zetknąć się z nowościami światowymi i dowiedzieć się, jakie rozwiązania będą stosowane w najbliższej przyszłości. Skorzystać mogą, i powinni, nie tylko specjaliści w dziedzinie systemów zabezpieczeń, projektanci, wykonawcy, eksperci i dystrybutorzy, ale także inwestorzy, konsultanci, autorzy norm i innych regulacji prawnych, które powinny nadążać za rozwojem technologicznym w tej dziedzinie.

Należy także przytoczyć opinię, którą podzielało wiele osób podczas dyskusji i rozmów kuluarowych – warto, aby taka impreza odbywała się cyklicznie, np. wiosną, co dwa lata, z udziałem liderów *security*, którzy za każdym razem będą mieli do zaprezentowania nowości technologiczne na światowym poziomie, oraz specjalistów z WAT, którzy także mają rozległą wiedzę na ten temat, nierzadko popartą własnymi badaniami i doświadczeniami.

Taka impreza, prezentująca rozwiązania nie starsze niż np. dwuletnie, miałaby szansę stać się elitarną, w najlepszym tego słowa znaczeniu.

Adam Bułaciński

GSM200
Wewnętrzny moduł GSM do centrali alarmowej PowerMax PRO

Co zrobić, gdy podłączenie standardowej linii telefonicznej do centrali alarmowej nie jest możliwe? Jak mieć zdalny dostęp do systemu alarmowego? Jak podłączyć do monitoringu obiekt, by otrzymywać informacje również na telefon komórkowy?

Odpowiedzią na wyżej postawione pytania jest nowy produkt firmy **Visonic GSM200.**

Jest to wewnętrzny moduł GSM, przeznaczony do współpracy z bezprzewodowymi centralami PowerMax PRO. Konstrukcję oparto na przemysłowym module GSM, umożliwiającym współpracę z dowolnym operatorem sieci komórkowej.

Niewielkie wymiary i kompaktowa budowa pozwalają na zamontowanie go wewnątrz obudowy centrali.

Dzięki rozbudowanym funkcjom GSM200 możemy: otrzymywać komunikaty głosowe lub SMS o stanie systemu, zdalnie sterować systemem z klawiatury dowolnego telefonu bądź wysyłając SMS-a, nawiązać dwukierunkową łączność głosową z osobą znajdującą się w obiekcie.

Firma **Visonic** nie zapomniała również o firmach monitorujących i wyposażyła GSM200 w funkcje przekazywania wszelkich sygnałów alarmowych w większości wykorzystywanych formatów telefonicznych. GSM200 może pracować jako urządzenie główne bądź jako zapasowe w przypadku awarii standardowej linii telefonicznej.

Bezpośr. inf. Visonic

AXS-5, AXS-100, TIAB
Elementy kontroli dostępu firmy Visonic

W swojej bogatej ofercie firma **Visonic** posiada również urządzenia do systemów kontroli dostępu. Najbardziej popularne spośród nich urządzenie **AXS-5** to prosty kontroler pojedynczego przejścia dla maksymalnie 25 użytkowników. Atrakcyjna cena w połączeniu z bardzo prostą instalacją charakteryzują produkt, który znajduje szerokie zastosowanie w małych i średnich obiektach. **AXS-100** to zaawansowany kontroler przejścia dwojga drzwi. Możliwość obsługi 5000 użytkowników, funkcja *Anti-passback,* możliwość połączenia w sieć kontrolerów obsługujących maksymalnie 200 przejść to funkcje, które umożliwiają instalację w najbardziej wymagających systemach kontroli dostępu. Złożoność **AXS-100** nie wyklucza łatwego procesu instalacji oraz obsługi. Czytelny wyświetlacz LCD ułatwia instalatorowi zapis kart i ogólny przegląd systemu. Kolejnym produktem jest **TAG-IN-A-BAG** (TIAB). Jest to kontroler pojedynczego przejścia z wbudowaną klawiaturą numeryczną. TIAB obsługuje do 250 kart zbliżeniowych, ma dwa tryby pracy: karta/karta + kod PIN, umożliwia podłączenie przycisku „wyjście alarmowe". Jest to bardzo funkcjonalne urządzenie,często wykorzystywane w średniej wielkości obiektach.

Bezpośr. inf. Visonic

5. Spotkanie Projektantów Instalacji Niskoprądowych w Ustroniu (5SPIN) – relacja

Pod skrótem 5SPIN kryje się piąta już konferencja przeznaczona dla projektantów i osób związanych z branżą instalacji niskoprądowych, zorganizowana przez firmę **Unima 2000 Systemy Teleinformatyczne** (Unima 2000) w dniach 4 i 5 października br. w Ustroniu (woj. śląskie).

W imprezie wzięło udział łącznie 122 osób, w tym 94 zaproszonych gości, 15 prelegentów, 11 osób z firmy Unima 2000, zajmujących się głównie koordynacją i organizacją konferencji, oraz dwie osoby reprezentujące prasę branżową i patronów medialnych (*Systemy Alarmowe* oraz *Zabezpieczenia*).

Na wstępie, w imieniu organizatorów oraz firm, które objęły imprezę patronatem, powitał uczestników konferencji Krzysztof Sikora, wiceprezes zarządu Unima 2000.

W pierwszym dniu konferencji zaprezentowano następujące referaty:

- „Światłowodowy i miedziany system okablowania strukturalnego" – Michał Wesołowski i Paweł Buńkowski, przedstawiciele firmy 3M, którzy pokazali m.in. gniazda sieciowe typu *one-click* z zaślepką przeciwkurzową oraz sieciowe rozwiązania światłowodowe i udzielili wielu cennych rad, związanych z projektowaniem, a także wykonawstwem okablowania strukturalnego;
- „Projektowanie zintegrowanych systemów bezpieczeństwa" – Tomasz Górski, przedstawiciel firmy TAP, który poprowadził część sprzętową, poświęconą centralom alarmowym Galaxy serii Classic i G3, oraz współpracujący z TAP Jerzy Taczalski z firmy Ifter, prezentujący podczas konferencji produkowane przez tę firmę oprogramowanie InPro do integracji systemów bezpieczeństwa;
- „Nowe rozwiązania w systemach kontroli dostępu – metody komunikacji oraz przykłady wdrożeń" – Paweł Pachela i Mirosław Kołda, przedstawiciele firmy Unicard, którzy mówili m.in. o sterownikach kontroli dostępu SD 2600 i modułach IO 2600, umożliwiających prostą i ekonomiczną rozbudowę systemu kontroli dostępu;
- „Autonomiczny radiowy system sygnalizacji pożaru IQ8Wireless firmy Esser" – Marcin Cichy, Krzysztof Kaniewski i Piotr Gronek z firmy Honeywell Life Security Austria Przedstawicielstwo w Polsce (w swojej ofercie firma posiada również inne systemy sygnalizacji pożaru Esser, dźwiękowe systemy ostrzegawcze Esser Sinaps oraz systemy komunikacji szpitalnej Ackermann Clino);
- „System zliczania ruchomych obiektów" – Jean-Francois Rheault z francuskiej firmy Eco Counter (referat tłumaczony na bieżąco z francuskiego przez Renatę Dudę z Unima), produkującej urządzenia do zliczania pieszych i rowerzystów na terenach rekreacyjnych, wykorzystujące czujniki piroelektryczne, akustyczne (zakopywane) oraz tuby pneumatyczne.

Drugi dzień konferencji rozpoczęła prezentacja firmy ADI przygotowana przez dr Janusza Kopacza z oddziału warszawskiego firmy ADI-Ultrak. Grupa ADI została powołana w 2005 roku do dystrybucji sprzętu z branży zabezpieczeń przez koncern Honeywell (ma w swojej ofercie produkty CCTV, SKDS, SSWiN, SSP oraz DSO).

Następnie przedstawiono trzy referaty tematyczne:

- „Unikalne właściwości i sposoby wykrywania pożaru" – Bernard Sokół, przedstawiciel firmy System Sensor, producenta oferowanych przez ADI czujek stosowanych w SSP, który omówił m.in. powody i konsekwencje fałszywych alarmów w SSP oraz wielosensorowe czujki COPTIR (Carbon Monoxide – Photoelectric –Termal – InfraRed);
- „Dźwiękowy system ostrzegawczy Ultrak SINAPS" – Jan Pacuk, który zwrócił uwagę na to, że zawarty w tym systemie wyniesiony mikrofon strażaka umożliwia łatwą obsługę nawet przez strażaka w rękawicach;
- „Systemy telewizji IP ADI-Ultrak" – Tomasz Mańturzyk, który omówił oferowane przez firmę produkty z tego zakresu, m.in. nowoczesny cyfrowy system monitoringu MatriVideo.

Ostatnie dwa referaty, dotyczące produktów amerykańskiej firmy Avaya, wygłosił Piotr Bac z firmy Unima 2000, po przedstawieniu historii swojej firmy:

- „Komunikacja w sieciach konwergentnych" – w referacie tym omówił produkt Avaya IP Office – platformę głosową dla średnich (zatrudniających 300–400 osób) firm, bazującą na nowoczesnej centrali telefonicznej wraz z oprogramowaniem aplikacyjnym;
- „Unified Communications – kiedy znikają granice pomiędzy technologiami" – referat ten dotyczył systemów ujednoliconej komunikacji firmy Avaya, umożliwiających usprawnienie realizacji procesów biznesowych w przedsiębiorstwie, m.in. dzięki zapewnieniu szybkiego i łatwego dostępu do pracowników, niezależnie od ich miejsca pobytu i używanego w celu komunikowania się urządzenia.

Na zakończenie organizator konferencji pożegnał uczestników i zaprosił na kolejne spotkanie w roku przyszłym.

Patronat nad imprezą sprawowały następujące firmy: 3M Poland, ADI-Ultrak, Avaya, Honeywell Life Security Austria, TAP, Unicard.

Adam Bułaciński

Razem już 25 lat

28 września odbyła się jubileuszowa uroczystość 25-lecia istnienia mikołowskiej firmy **Kabe**. W drzwiach lokalu, oprócz witających prezesów: **Kazimierza Bulandry** i **Grzegorza Krupy,** czekała urocza hostessa wręczająca drobne łakocie panom oraz kelner z różami dla wchodzących pań.

Po oficjalnym przywitaniu nastąpiły gratulacje ze strony gości: posła, starosty, burmistrza oraz zaprzyjaźnionych z firmą kontrahentów.

Jubileusz firmy uświetnił koncert zespołu Carrantuohill, wykonującego tradycyjną muzykę celtycką (zdobywcy Fryderyka 2006). Chętnych do tańczenia wprawdzie nie było, ale wszystkim nogi podskakiwały pod stołami… Dodatkowym irlandzkim akcentem były kilty, w których wystąpili kelnerzy. Mamy nadzieję, że taką małą Irlandię uda nam się stworzyć w Kabe i młodzi ludzie nie będą wyjeżdżali do pracy za granicę.

Pierwszy kawałek tortu ukroili współwłaściciele i ich żony. Do kawy podano ciasteczka zawierające wróżby, więc każdy mógł sprawdzić, co dobrego mu się przytrafi albo jakie będą szczęśliwe numerki w Lotto.

Obejrzeliśmy również prezentację przedstawiającą historię 25-lecia działalności firmy, przygotowaną przez pracowników. Najkrócej pracujący dowiedzieli się, jak duet prezesów zaczynał działalność w piwnicy jednego z nich, jak sami zaczęli wyjeżdżać po towar za granicę, aż w końcu przeprowadzili się do własnego budynku o powierzchni 1200m^2. Obaj prezesi wręczyli dyplom dla „Najwytrwalszego Kabowca" Jurkowi Czarnocie, który pracuje w firmie już od 1988 roku. Odbył się też konkurs „Wiedzy o Kabe". Pytania nie były łatwe, ale drużyny dzielnie walczyły o pierwsze miejsce.

Prezesi dostali piękne zdjęcie, na którym są wszyscy pracownicy. Nie mogli wyjść z podziwu, jak w tym celu udało się nam w tajemnicy zebrać przed siedzibą firmy.

Skocznym, irlandzkim krokiem wracaliśmy do domu, dyskutując o tym, co było, i zastanawiając się, jak uczcimy za 5 lat kolejny jubileusz Kabe. Będzie fantastycznie – nikt nie wątpi!!!

Bezpośr. inf.
Ewa Krupa-Herbska
Kabe

Urządzenia do zamgławiania w ofercie AWC Protect Global

Firma **AWC Protect Global System Polska** wprowadza do swojej oferty nowe urządzenie duńskiej firmy Protect o nazwie **SMS Fog Cannon**, służące do zamgławiania.

Urządzenie jest połączeniem działka dymnego, nadajnika SMS i czujnika PIR. Alarm jest uruchamiany i wyłączany poprzez wysłanie SMS-u. Tą drogą użytkownik otrzymuje również informację o włamaniu oraz inne informacje o aktualnym statusie urządzenia.

Więcej informacji na str. 76

Bezpośr. inf. AWC Protect Global System Polska

Softex Data spółką akcyjną

5 października w siedzibie elitarnego klubu przedsiębiorców Business Centre Club prezes zarządu firmy **Softex Data, Wojciech Warski**, uroczyście poinformował zaproszonych gości o zmianie formy własności na spółkę akcyjną (Softex Data jest spółką akcyjną od 1 lipca 2007 roku). Przedstawił w skrócie zakres działania i osiągnięcia firmy oraz zapewnił, że będzie ona nadal zapewniać indywidualne podejście do klienta oraz wysoką jakość sprzedawanych produktów i świadczonych usług. Wojciech Warski zaprezentował również oficjalnie **nowe logo spółki.**

Od momentu powstania, w 1990 roku, przez 16 lat Softex Data była firmą całkowicie prywatną. Decyzja o zmianie formy własności miała na celu zwiększenie zaufania klientów i partnerów do firmy oraz umożliwienie sprzedaży akcji spółki inwestorowi finansowemu. Pozyskane w ten sposób fundusze Softex Data planuje przeznaczyć na rozwój działalności związanej z bezpieczeństwem teleinformatycznym.

W imprezie uczestniczyło około 50 gości (prezesi i dyrektorzy firm oraz dziennikarze).

Po części oficjalnej wystąpił młody iluzjonista Łukasz Wiśniewski, który swoimi trikami wywołał rozbawienie oraz podziw. W zorganizowanej loterii fantowej można było wygrać markowe wino lub koniak.

Na zakończenie imprezy goście zostali zaproszeni na wykwintny bankiet, podczas którego w przyjaznej atmosferze, przy lampce wybornego wina kontynuowano rozmowy.

O firmie:

Początkowo firma Softex zajmowała się pisaniem oprogramowania, następnie do oferty weszły tzw. drukarki ciężkie i wysokowydajne, które zamawiane były przez większość działających w Polsce banków. To był strzał w dziesiątkę. Firma odnotowała znaczące zyski, które przeznaczyła między innymi na dalszy rozwój. Z czasem wprowadzono do oferty system archiwizacji i zarządzania dokumentami oraz urządzenia do systemów monitoringu.

„Softex Data aktywnie uczestniczy w życiu gospodarczym i społecznym. Jako dystrybutor urządzeń do monitoringu jest członkiem Polskiej Izby Systemów Alarmowych. Dzięki ścisłej współpracy z firmą Printronix działa w prestiżowym gronie amerykańskich przedsiębiorstw skupionych w American Chamber of Commerce. Nie pozostaje także obojętna na problemy społeczne. Stale pomaga szkole podstawowej w Sękowej, rokrocznie wspiera Wielką Orkiestrę Świątecznej Pomocy oraz uczestniczy w społecznych inicjatywach American Chamber of Commerce i Business Centre Club".

(źródło: mat. firmowe).

Teresa Karczmarzyk

Dyskretna ochrona

Nowe kamery wewnętrzne firmy Axis to najlepsza propozycja dyskretnej ochrony obiektów.

Dwa kolejne modele sieciowych kamer z popularnej linii Fixed Doom – **Axis 209FD** (VGA) oraz **Axis 209MFD** (megapikselowa) – oferują doskonałą jakość obrazu. Można je łatwo i szybko zainstalować na trudno dostępnych powierzchniach.

Niewielkich rozmiarów kamery, mierzące zaledwie 4 cm wysokości, zawierają w sobie najnowocześniejsze technologie: progresywne skanowanie, równoczesne przesyłanie dwustrumieniowe: Motion JPEG i MPEG-4, możliwość zasilania PoE i wiele innych. Axis zapewnia wysoki poziom bezpieczeństwa poprzez zastosowanie wielopoziomowego zabezpieczenia hasłami, filtrowanie adresów IP i możliwość przesyłu danych w szyfrowanym standardzie HTTPS.

Kamery Axis idealnie sprawdzają się w sklepach, hotelowych recepcjach, na korytarzach i we wszystkich wnętrzach, w których wymagana jest dyskretna ochrona.

Autoryzowanym dystrybutorem Axis w Polsce jest Softex Data.

Bezpośr. inf. Softex Data

Bezpieczne **Święta**

zapewniają urządzenia do systemów alarmowych Satel

Z okazji zbliżających się Świąt Bożego Narodzenia pragniemy życzyć Państwu dużo spokoju, rodzinnej atmosfery oraz wielu sukcesów

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

Aspekty monitorowania bezpieczeństwa wewnątrz dużych instytucji finansowych

Każda instytucja stara się chronić własne zasoby w sposób, który, jej zdaniem, jest jak najbardziej dla niej odpowiedni. Zdrowie i życie są wartościami, których przecenić nie można. Pozyskana w nieuprawniony sposób informacja, czasem pozornie mało istotna, umiejętnie wykorzystana przez osoby żądne zysku, może kosztować daną firmę mnóstwo pieniędzy, o utracie dobrego imienia nie wspominając. Straty spowodowane zagarnięciem mienia mogą zostać zrekompensowane przez ubezpieczyciela, pod warunkiem, że zapewniony został odpowiedni poziom zabezpieczenia chronionych zasobów

Banki są tym rodzajem instytucji finansowych, w których życie i zdrowie klientów oraz pracowników, a także informacja oraz mienie, narażone są na działanie osób, które kierują się chęcią szybkiego wzbogacenia się w sposób niekoniecznie zgodny z prawem. Stosowane powszechnie systemy zabezpieczeń informatycznych, elektronicznych czy mechanicznych nie zawsze są w stanie ostudzić zapał tych, którzy, nie bacząc na grożące im konsekwencje, pragną wzbogacić się w szybki sposób. Dlatego aby móc podejmować zdecydowane i trafne działania już w chwili wystąpienia zdarzenia alarmowego, a dodatkowo mieć możliwość prowadzenia długofalowych analiz,

których celem będzie realizacja skutecznych działań korygująco-naprawczych, konieczne jest prowadzenie stałego monitorowania stanu bezpieczeństwa zasobów objętych ochroną.

W Departamencie Bezpieczeństwa PKO Banku Polskiego wyodrębniony został Wydział Monitorowania i Zarządzania Systemami Bezpieczeństwa, w zakresie kompetencji którego jest m.in. prowadzenie działań związanych z monitorowaniem bezpieczeństwa i ochrony osób i mienia, systemu informatycznego oraz informacji prawnie chronionych. Takie zadania, jak:

- bieżący monitoring systemów zabezpieczeń elektronicznych i mechanicznych,
- monitorowanie bezpieczeństwa systemów IT,
- nadzór i weryfikacja realizacji usług z zakresu bezpieczeństwa, świadczonych na rzecz banku przez podmioty zewnętrzne (m. in. serwis i konserwacja systemów zabezpieczeń elektronicznych, zabezpieczeń mechanicznych, realizacja transportu i ochrony wartości pieniężnych, monitorowanie sygnałów alarmowych wraz z interwencją załóg patrolowych),

realizowane są przez kilka zespołów specjalistów i są prowadzone w różnych systemach pracy, w zależności od ich stopnia krytyczności (całodobowo, w trybie dwu- i jednozmianowym). W strukturze wydziału funkcjonuje Centralny Ośrodek Monitorowania Bezpieczeństwa (COMB), w którym zadania prowadzone są w systemie całodobowym. Ośrodek realizuje zadania z zakresu monitorowania, obejmując swoim zasięgiem cały kraj.

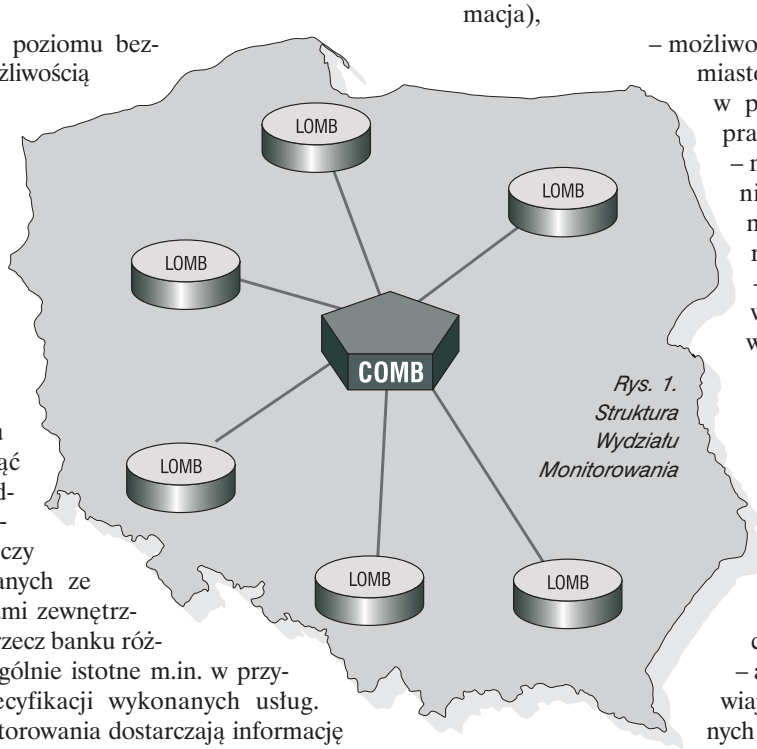
Obecnie bank posiada ok. dwóch tysięcy obiektów (oddziały banku, bankomaty zewnętrzne, inne budynki), z których każdy objęty jest ochroną (systemy zabezpieczeń, monitorowanie wraz z interwencją, w niektórych obiektach posterunki stałej ochrony fizycznej). W obiektach tych pracownicy podmiotów zewnętrznych – z którymi bank ma podpisane umowy – realizują zadania m.in. z zakresu serwisu i konserwacji systemów informatycznych oraz zabezpieczeń technicznych i mechanicznych, co powoduje, iż mają dostęp do mienia banku, a także informacji o krytycznym dla niego znaczeniu. W banku pracownicy realizują swoje zadania na przeszło 30 tysiącach komputerów (ta liczba obejmuje również serwery, na których działają ważne dla banku aplikacje), a niewłaściwe wykorzystanie któregokolwiek z nich może być bardzo groźne dla wewnętrznej sieci banku. Także podłączenie do sieci komputerowej nieuprawnionego urządzenia i wykonanie za jego pomocą ataku „z wewnątrz" mogłoby spowodować ogromne straty. Wszystko to sprawia, iż w tak dużej instytucji niezwykle

istotny jest nie tylko odpowiedni poziom zabezpieczeń, uniemożliwiający nieuprawnione działania, lecz również natychmiastowa informacja o wystąpieniu – bądź nawet próbie – naruszenia bezpieczeństwa, i to z dokładnością do konkretnego punktu, jest bardzo ważna dla służb, które odpowiadają za bezpieczeństwo. Takie podejście do problemu pozwala na podejmowanie przez nie (na podstawie opracowanych wcześniej procedur) natychmiastowych działań naprawczych już w momencie wystąpienia zdarzenia. Prowadzona statystyka wystąpień nieprawidłowości umożliwia wyznaczenie trendów, a ich analiza jest podstawą przy podejmowaniu działań eliminujących możliwość wystąpienia w przyszłości zdarzeń z danej grupy ryzyka.

Fot.1. Centralny Ośrodek Monitorowania Bezpieczeństwa

Prowadzenie skutecznych działań związanych z monitorowaniem bezpieczeństwa w tak rozbudowanej pod względem terytorialnym i organizacyjnym instytucji nie byłoby możliwe dzięki funkcjonowaniu wyłącznie jednego Centralnego Ośrodka Monitorowania Bezpieczeństwa. W strukturze wydziału monitorowania działają również Lokalne Ośrodki Monitorowania Bezpieczeństwa, które – realizując zadania w systemie dwuzmianowym – wspierają działania podejmowane przez COMB na terenie przypisanego im obszaru terytorialnego.

Stałe monitorowanie poziomu bezpieczeństwa – poza możliwością posiadania informacji o nieprawidłowościach już w momencie ich wystąpienia – ma jeszcze inne zalety, dzięki którym można osiągnąć oszczędności. Każda informacja, która trafi do systemów monitorowania, jest zapisywana w bazie danych, dzięki czemu można do niej sięgnąć każdorazowo w przypadku wystąpienia jakichkolwiek wątpliwości czy niejasności, np. związanych ze współpracą z podmiotami zewnętrznymi, realizującymi na rzecz banku różne usługi. Jest to szczególnie istotne m.in. w przypadku rozliczania specyfikacji wykonanych usług. Dane z systemów monitorowania dostarczają informację o momencie wystąpienia awarii (np. systemu sygnalizacji włamania i napadu), czasie dotarcia pracownika serwisu do obiektu (zgłoszenie obiektu „w serwis"), a także czasie realizacji usługi (zgłoszenie „gotowości obiektu"). Weryfikacja poprawności wykonanej usługi dokonywana jest zarówno za pomocą systemów monitorowania (zweryfikowanie, czy sygnał awarii w danym obiekcie jeszcze występuje), jak i, wyrywkowo, w przypadku niektórych obiektów – na miejscu. Taki sposób działania pozwala na wyeliminowanie nieprawidłowości w specyfikacjach wykonanych usług, a pracownicy podmiotów zewnętrznych, świadomi prowadzonych przez zlecającego działań, wykazują się większym zaangażowaniem w realizację usług.



Rys. 1. Struktura Wydziału Monitorowania

Reasumując, prowadzenie własnych działań związanych z monitorowaniem bezpieczeństwa, m.in. w instytucjach finansowych, ma wiele korzyści, na które składają się:

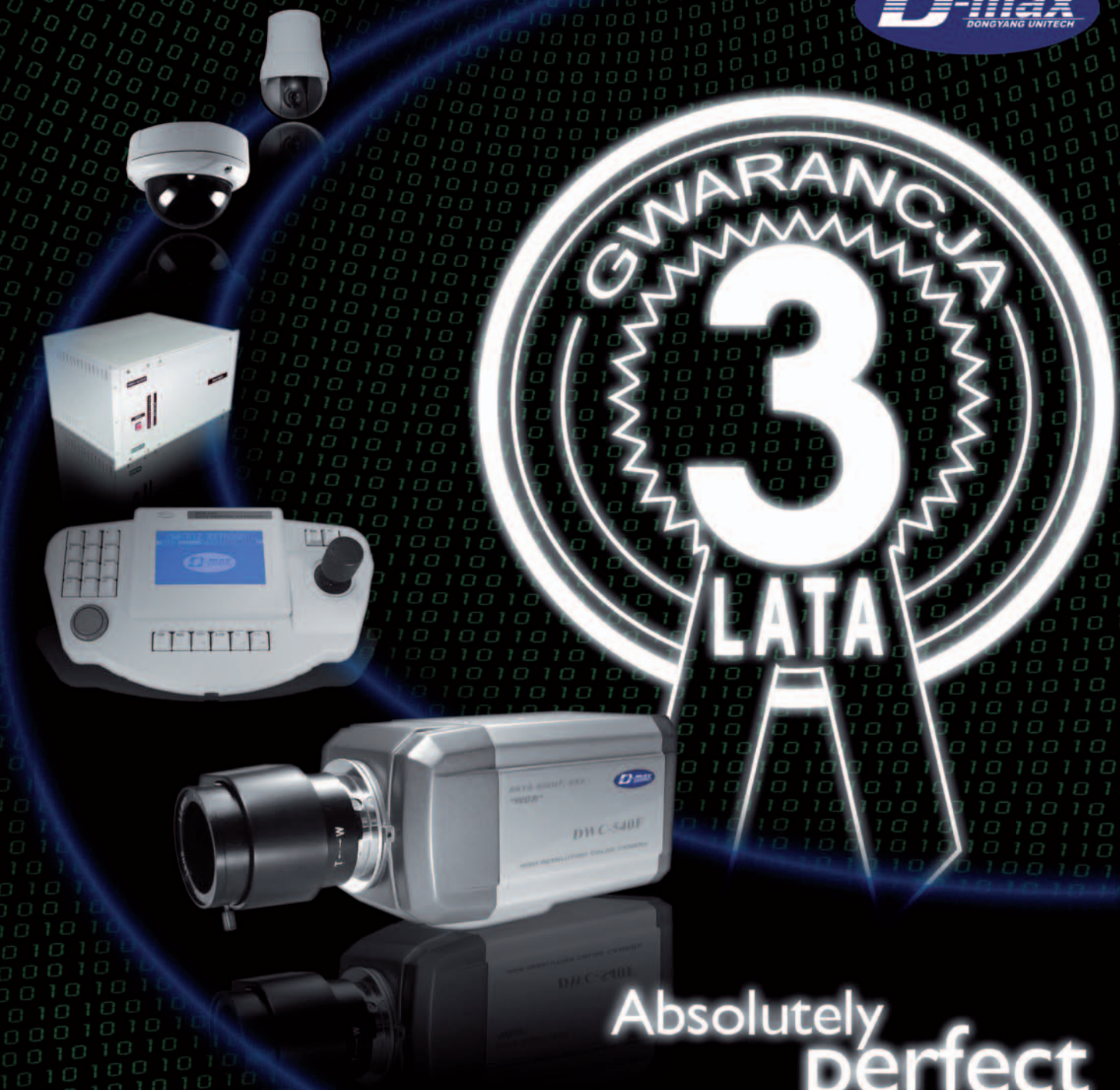
– podniesienie poziomu bezpieczeństwa chronionych zasobów (ludzie, gotówka, zasoby informatyczne, informacja),
– możliwość podejmowania natychmiastowych kroków naprawczych w przypadku wystąpienia nieprawidłowości,
– natychmiastowe informowanie o poważnych naruszeniach bezpieczeństwa kierownictwa,
– koordynacja działań służb wewnętrznych w przypadku wystąpienia zagrożenia bezpieczeństwa,
– podniesienie jakości usług realizowanych przez podmioty zewnętrzne,
– jednoznaczna rozliczalność realizacji usług,
– krótkoterminowa analiza raportów, pozwalająca na klasyfikację i prezentację zdarzeń alarmowych,
– analiza długofalowa, umożliwiająca podejmowanie efektywnych działań korygująco-naprawczych, określenie trendów.

Konsekwencją tych korzyści są oszczędności w zakresie budżetu kosztowego dla instytucji.

Krzysztof Białek
Naczelnik Wydziału Monitorowania i Zarządzania Systemami Bezpieczeństwa Departament Bezpieczeństwa PKO Bank Polski

ZAAWANSOWANY SYSTEM MONITORINGU

D-max DONGYANG UNITECH



Absolutely perfect

ALPOL HURTOWNIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

ALPOL Sp. z o.o.
ul. H. Krahelskiej 7
40-285 Katowice
tel.: 0 32 790 76 56
fax: 0 32 790 76 61
email: alpol@e-alpol.com.pl
www: www.e-alpol.com.pl

VCN
ul.Kraszewskiego 21/25
60-501 Poznań
tel.: 0 61 622 94 92
fax: 0 61 622 94 95
email: biuro@vcn.pl
www: www.vcn.pl

ProfiCCTV
ul. Heleny Szafran 10
60-179 Poznań
tel.: 0 61 842 29 62
fax: 0 61 842 29 62
email: dmax@dmaxcctv.pl
www: www.dmaxcctv.pl

Fonex SYSTEMY ZABEZPIECZEŃ
Przedsiębiorstwo FONEX
ul. Armii Krajowej 1/3
42-200 Częstochowa
tel.: 0 34 365 33 82
fax: 0 34 368 12 10
email: biuro@fonex.com.pl
www: www.fonex.com.pl

PAW SYSTEMY ZABEZPIECZEŃ
PAW Systemy Zabezpieczeń
ul. Morska 65
81-323 Gdynia
tel.: 0 58 620 07 21
email: pw-paw@o2.pl
www: www.pawalarmy.pl

System Floodline

System firmy Andel do wykrywania i monitoringu wycieków ROZWIĄZANIA

Skuteczność wykrywania zagrożeń spowodowanych wszelkiego rodzaju wyciekami zależy od wielu czynników. W praktyce najlepiej sprawdzają się systemy strefowe

W systemach wykrywania wycieków stosowane są dwa podstawowe rozwiązania różne co do filozofii detekcji. System Long Line, skonstruowany w USA, a następnie powielany w innych systemach, był dotychczas jedynym tego typu rozwiązaniem dostępnym na naszym rynku. Polega on na technice kumulacji rezystancji. Sygnalizator lokacji systemu Long Line podaje odległość miejsca wycieku od punktu zerowego. System ten nadaje się najlepiej do nadzorowania długich, prostych odcinków, jest stosunkowo łatwy do zaprojektowania, a lokalizacja miejsca wycieku podawana jest z dokładnością do jednego metra. Nie jest on niestety pozbawiony wad. Do najistotniejszych należy zaliczyć: brak możliwości uzyskania dokładnych informacji na temat miejsca wycieku, brak możliwości wykrywania kilku wycieków w tym samym czasie, trudną modyfikację i rozbudowę, konieczność ponownego wzorcowania po każdej zmianie.

Pozbawiony wyżej wymienionych wad jest system strefowy.

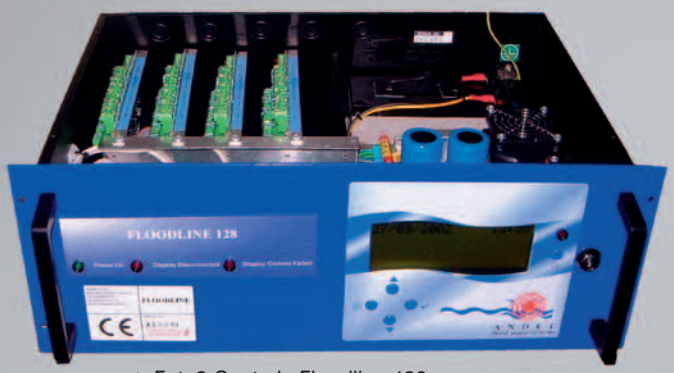
W systemie tym miejsce wycieku przypisane jest do określonej strefy, którą może być pomieszczenie, odcinek rurociągu, urządzenie itp.

Ze względu na to, że poszczególne strefy są od siebie odseparowane, możliwe jest wykrywanie wielu wycieków jednocześnie. Rozwiązanie takie jest szczególnie pomocne przy kontrolowaniu większych awarii poprzez śledzenie szybkości i kierunku ich rozwoju. Budowa modułowa umożliwia rozbudowę systemu w każdej chwili, tak aby można było dostosować go do aktualnych potrzeb. W systemie Floodline strefy mogą stanowić odcinki przewodu wielostrefowego detekcyjnego, czujki punktowe, czujki dywanowe (fot. 1), taśmy detekcyjne, czujki specjalne (fot. 2). Przewody wielostrefowe, stosowane w układach detekcyjnych, mogą, w zależności od potrzeb, występować w wersji cztero- lub ośmiostrefowej. Łączenie odcinków przewodów detekcyjnych odbywa się w bardzo łatwy sposób, za pomocą modułów (SOL, Autocoupler) i złączek typu Rj. Można zdecydować się na zamówienie u dystrybutora przewodów detekcyjnych gotowych do podłączenia, o dowolnej długości, lub przygotowywać je i uzbrajać w zaciski dopiero na budowie. Łączenie przewodów za pomocą modułów i złączek pozwala na bardzo łatwy demontaż przewodu w celu jego oczyszczenia, osuszenia po zalaniu itp.

Występujące w ofercie firmy Andel czujki punktowe wykonane są w wersjach do montażu poziomego lub pionowego. Dzięki wyposażeniu ich w osłony wykonane ze stali nierdzewnej są one odporne na uszkodzenia mechaniczne, co zwiększa ich niezawodność. Taśmy detekcyjne i maty dywanowe stosowane są przypadku, gdy wymagana jest bardzo wysoka czułość układu – nawet niewielka zmiana wilgotności lub obecność pary wodnej jest przez nie wykrywana. Czujki specjalne mają zastosowanie w przypadkach, gdy zastosowanie wyżej wymienionych elementów jest niemożliwe, np. wewnątrz zbiorników. Aby można było dostosować system do potrzeb każdego klienta, do dyspozycji jest szeroka gama central. Występują one w wersjach 1-, 2-, 4-, 8-, 16- i 32-strefowych. Dla większych aplikacji stosuje się centrale 128-strefowe, które, dzięki ich modułowej budowie, można odpowiednio konfigurować, uzyskując wymaganą pojemność – od 32 do 128 stref. Centrala Floodline, 128-strefowa, może również zostać zabudowana w standardowej szufladzie 19” do montażu w szafie typu „Rack” (fot. 3). Na wbudowanym ciekłokrystalicznym wyświetlaczu można uzyskać precyzyjne tekstowe informacje, określające miejsce, rodzaj i czas zdarzenia.

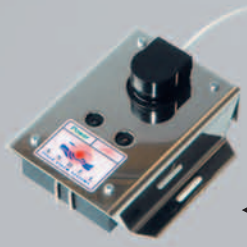
Wszystkie centrale wykrywają i sygnalizują wszelkie nieprawidłowości i uszkodzenia systemu oraz jego elementów, stan zasilania podstawowego i awaryjnego akumulatorowego, jak również umożliwiają przesyłanie sygnałów do systemów

Elementy systemu wykrywania wycieków



▲ Fot. 3 Centrala Floodline 128

◄ Taśma detekcyjna



Fot. 1 ► Czujka specjalna

◄ Fot. 4 Moduł Groundhog

Fot. 2 ► Czujka dywanowa

nadrzędnych (np. BMS) lub systemów monitorujących. Wewnętrzna pamięć centrali umożliwia zapamiętanie 250 ostatnich zdarzeń z określeniem ich miejsca i czasu.

Na uwagę zasługują także proste jednostrefowe rozwiązania typu Leak 1 Mk II oraz Groundhog. Moduł Leak 1 Mk II jest przeznaczony do montażu na szynie DIN i może być zastosowany jako uzupełnienie innych systemów kontrolujących/alarmowych instalowanych w budynku, np. SSWiN. Możliwe jest podłączenie do niego zarówno czujki punktowej, przewodu lub taśmy detekcyjnej.

Z kolei moduł Groundhog (fot. 4) stanowi niezależną jednostkę z czujką punktową do montażu na posadzce, wyposażoną w sygnalizację optyczną i wyjście alarmowe.

Jak widać, system Floodline jest niezwykle funkcjonalny i elastyczny. Dzięki szerokiej gamie paneli sterujących i czujek można go dostosować do występujących potrzeb, co jest niezwykle istotne ze względu na możliwość optymalizacji kosztów.

Konstrukcja systemu jest oparta na wieloletnich doświadczeniach producenta. Dzięki zastosowaniu w nim najnowocześniejszych rozwiązań technicznych uzyskano dużą skuteczność działania i bardzo wysoką odporność na zakłócenia, a tym samym ograniczenie występowania fałszywych alarmów. Niepodważalnym argumentem przemawiającym za powszechnym stosowaniem systemu Floodline są niewielkie koszty jego instalacji i eksploatacji.

Arkadiusz Milka

Autor jest prezesem zarządu P. U. T. „Intel”, generalnego dystrybutora systemu Floodline w Polsce

Szczegółowe informacje:
tel. 012 411-49-79
e-mail: intel@intel.net.pl

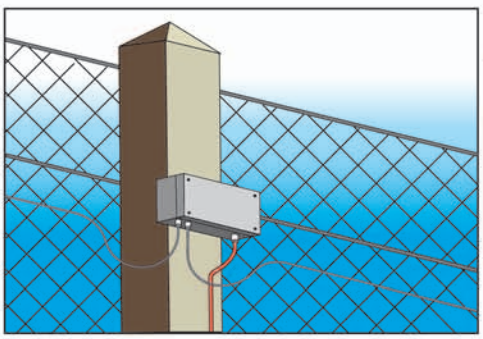
firma ATLine®

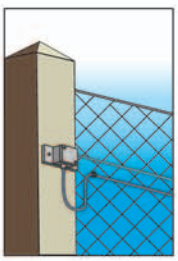
Firma ATLine spółka jawna
91-845 Łódź, ul. Franciszkańska 125
tel. +48 042 657 30 80, fax +48 042 655 20 99
e-mail: info@atline.pl
www.atline.pl

Liniowy czujnik wibracyjny na ogrodzenie
– konfiguracja na 600m:

klasa

AN 303 – sterownik czujnika wibracyjnego • 2 strefy po 300m, • 2 terminatory do zakończenia stref	1 szt. x 4 150,- zł = 4 150,- zł netto
AS 257 – kabel sensoryczny do systemu AN	600 m x 8,30 zł = 4 980,- zł netto





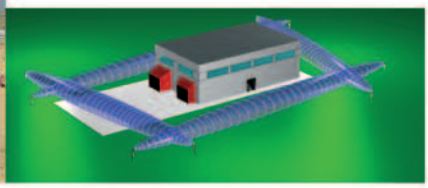
PIRAMID XL2
zewnętrzna, dualna czujka procesowa, z możliwością regulacji czułości PIR i MW oraz położenia.

• **szeroki kąt:** SDI-76 XL2 (kąt 15m x 15m) SDI-77 XL2-A (kąt 27m x 15m) • **średni kąt:** SDI-77 XL2-B (kąt 30m x 10,5m) • **wąski kąt:** SDI-77 XL2-C (kąt 37,5m x 6m) SDI-77 XL2-D (kąt 30m x 3m)	2 830,- zł netto

ERMO 482
bariera mikrofalowa do zewnętrznej ochrony obwodowej konfiguracja na 4 strefy po 50 m:

klasa

ERMO 482/50 – zewn. bariera mikrofalowa do 50 m (nadajnik i odbiornik)	4 kpl. x 2 386,- zł = 9 544,- zł netto
PALO VERDE – słupek do bariery Ermo, ze stali nierdzewnej, malowany proszkowo • fi 60mm, h=1,9m	8 szt. x 195,- zł = 1 560,- zł netto
• ERMO 482 - bariera analogowa, • ERMO 482X PRO - bariera cyfrowa z analią przebiegu sygnału. Dostępne zasięgi: 50, 80, 120 lub 200 metrów.	



GPS
niewidoczny, zakopywany system ochrony obwodowej

Zestaw na 1 strefę 100 m (w tym dwa kable ciśnieniowe)	22 800,- zł netto

Niewidoczny, zakopywany system GPS Plus wykrywa zmiany nacisku na grunt jakie powoduje wtargnięcie intruza w chroniony obszar. System ignoruje małe zwierzęta, ptaki i zakłócenia pogodowe, ponadto jest całkowicie nieczuły na działanie pola elektromagnetycznego. Temperatura pracy: od -40°C do +70°C.

artykuł sponsorowany

Urządzenia, które się sprawdzają

GPRS-N, GPRS-D
Nowe nadajniki firmy Pulson

Od momentu uruchomienia pierwszej komercyjnie działającej sieci telefonii komórkowej w cyfrowym standardzie GSM w Polsce minęło już 11 lat. W tym czasie operatorzy rozwinęli swoje sieci tak, że można już mówić o zasięgu globalnym w skali kraju. Równolegle z rozbudową infrastruktury poprawiła się jakość podstawowych usług i wprowadzano nowe, oparte na transmisji danych. Rozszerzenie technologii pakietowej transmisji danych GPRS do standardu EDGE oraz wprowadzenie całkowicie nowej technologii UMTS pozwoliło znacznie zwiększyć szybkości przepływu informacji. Jednocześnie podstawowy standard GPRS jest obecnie osiągalny wszędzie tam, gdzie mamy zasięg sieci GSM, co pozwoliło stworzyć wiele nowych aplikacji, wykorzystujących pakietową transmisję danych

Transmisja danych GPRS, obok krótkich wiadomości tekstowych SMS oraz funkcji identyfikacji numeru dzwoniącego CLIP, stała się medium dla urządzeń służących do przesyłania sygnałów alarmowych z obiektów chronionych do centrum monitoringu. Oprócz znacznego obniżenia kosztów w stosunku do transmisji SMS, system wykorzystujący pakietową transmisję danych posiada bardzo istotną cechę – pozwala na komunikację w „czasie rzeczywistym". Dzięki temu jego wiarygodność jako całości zwiększa się, ponieważ istnieje możliwość znacznie częstszej kontroli łącza.

Przykładem kompleksowego rozwiązania takiego systemu jest opracowana i produkowana w firmie Pulson stacja SMSCI wraz z nadajnikami abonenckimi, pracującymi w trybie transmisji danych GPRS. System ten jest rozwinięciem oferowanego wcześniej przez firmę rozwiązania opartego na transmisji SMS/CLIP. Opis nowej stacji SMSCI był tematem artykułu zamieszczonego w numerze 4(56)/2007 czasopisma *Zabezpieczenia*. Poniższy tekst prezentuje część nadawczą systemu – **moduły nadawcze GPRS-N** i **GPRS-D**.

Tryby pracy

Nadajniki GPRS-N i GPRS-D zostały zaprojektowane do współpracy z centralami alarmowymi. Zbudowane są na bazie specjalizowanych układów mikroprocesorowych, wyposażone w przemysłowy modem GSM/GPRS i zamknięte razem z układem zasilania w zwartej metalowej obudowie.

Działanie modułów nadawczych opiera się na usługach transmisji danych GPRS oraz SMS i CLIP, realizowanych w sieci telefonii komórkowej GSM. Informacje o stanie monitorowanego obiektu przesyłane są za pomocą pakietowej transmisji danych, wiadomości SMS lub informacji o numerze, z którego jest wykonywane połączenie – tzw. CLIP. Raporty te docierają do urządzenia odbiorczego SMSCI zainstalowanego w stacji monitorowania obiektów, gdzie są odpowiednio identyfikowane i rejestrowane.

Nadajniki umożliwiają pracę w dwóch trybach – „GPRS" lub „GSM". W trybie pracy GPRS informacje o zdarzeniach wysyłane są poprzez sieć pakietowej transmisji danych operatora w postaci zaszyfrowanej ramki, z wykorzystaniem protokołu UDP. Docierają one do określonego numeru IP stacji odbiorczej SMSCI, zainstalowanej w centrum monitorowania, gdzie po rozszyfrowaniu dekodowane są dane o numerze abonenta i zdarzeniu. Każda informacja wysłana przez nadajnik wymaga potwierdzenia odbioru sygnału przez stację. W przypadku jego braku nadajnik może powtórzyć wysyłanie i w razie niepowodzenia automatycznie przełączyć się w tryb GSM, by wysłać zdarzenie w postaci SMS. Tego rodzaju praca zwiększa prawdopodobieństwo dostarczenia informacji.

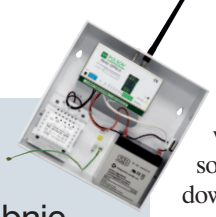
W trybie pracy GSM raporty SMS z nadajników docierają do stacji SMSCI poprzez odbiorcze karty GSM zainstalowane w stacji lub za pośrednictwem łącza z SMSC operatora telefonii komórkowej.

Oprócz stacji monitorowania moduł nadajnika może automatycznie informować właściciela obiektu lub inną upoważnioną osobę o wybranych zdarzeniach zaistniałych w obiekcie.

Budowa i właściwości

Moduły nadawcze GPRS-N i GPRS-D analizują stan niezależnych wejść alarmowych typu NO/NC, do których można podłączyć wyjścia logiczne central alarmowych i czujnik sabotażu obudowy. Zmiana stanu dowolnego wejścia powoduje wygenerowanie zaprogramowanego, dwuznakowego kodu zdarzenia i wysłanie go w postaci pakietu UDP lub komunikatu SMS do stacji odbiorczej SMSCI.

Moduł nadawczy GPRS-D ma również możliwość bezpośredniej komunikacji z dialerami central alarmowych poprzez wbudowany symulator linii telefonicznej i odbiornik transmisji DTMF w formacie Contact ID. Dekodowane raporty DTMF z centrali przesyłane są do stacji SMSCI w formie dziewięcioznakowych kodów zdarzeń.



Zastosowane rozwiązania układowe sprawiają, iż jest to prawdopodobnie jedyny na rynku tego typu nadajnik, zapewniający poprawną współpracę z większością central alarmowych.

Dwa niezależne wyjścia przekaźnikowe umożliwiają zdalne (z uprawnionych numerów) załączanie lub wyłączanie urządzeń w obiekcie monitorowanym. Wyjście 1 może być załączane automatycznie, na określony czas, w momencie zmiany stanu wybranego wejścia alarmowego NO/NC. Wyjście 2 może służyć do „sygnalizacji awarii". W przypadku problemów z zalogowaniem do sieci GSM pozwala automatycznie załączyć inny tor transmisji lub zasygnalizować awarię.

Urządzenia posiadają własny zasilacz sieciowy, który ładuje akumulator. Dla poprawnej pracy wymaga on napięcia przemiennego 18 V z transformatora. Nadajnik testuje obecność napięcia i w przypadku jego zaniku lub powrotu sygnalizuje zdarzenie zaprogramowanym dwuznakowym kodem. Obecność zasilania sieciowego jest sygnalizowana czerwoną diodą LED.

Wyjścia przekaźnikowe, wejścia alarmowe i wejścia zasilania przyłączane są poprzez zaciski śrubowe. Dodatkowo urządzenia posiadają złącze służące do programowania ustawień z komputera i gniazdo karty SIM. Tryb pracy nadajników sygnalizują dwie diody LED. Na górnej ściance obudowy znajduje się gniazdo antenowe w standardzie FME.

Całość przystosowano do zamocowania w skrzynce z transformatorem firmy PULSAR typu AWO 033.

Transmisja ContactID

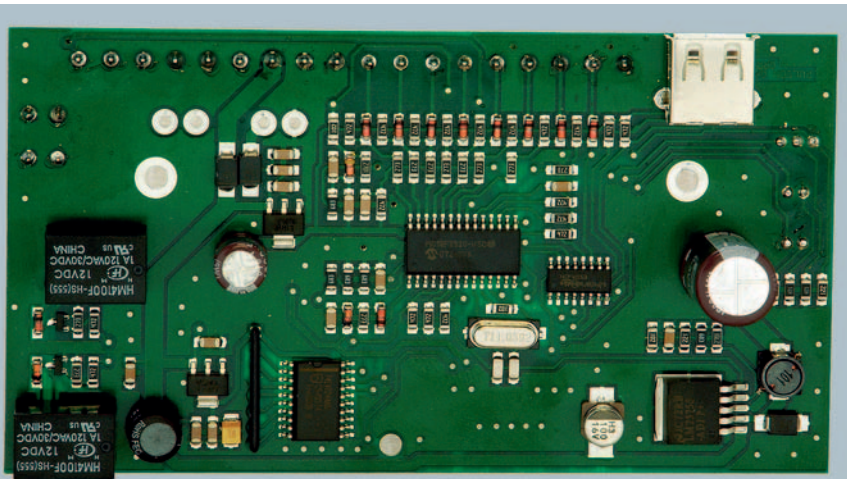
Nowością w opisywanym systemie jest możliwość transmisji przez nadajnik GPRS-D dziewięcioznakowych zdarzeń w formacie Contact ID, odbieranych bezpośrednio z centrali alarmowej.

GPRS-D został wyposażony w symulator linii telefonicznej i odbiornik transmisji DTMF w formacie Contact ID. Odbiornik realizuje pełen protokół zestawiania połączenia centrali alarmowej ze stacją odbiorczą – generuje sygnał inicjujący, odbiera depeszę DTMF i kończy transmisję, nadając sygnał zakończenia. Z punktu widzenia centrali nadajnik GPRS-D jest stacją odbiorczą systemu monitorowania telefonicznego, zgodną ze standardem Contact ID.

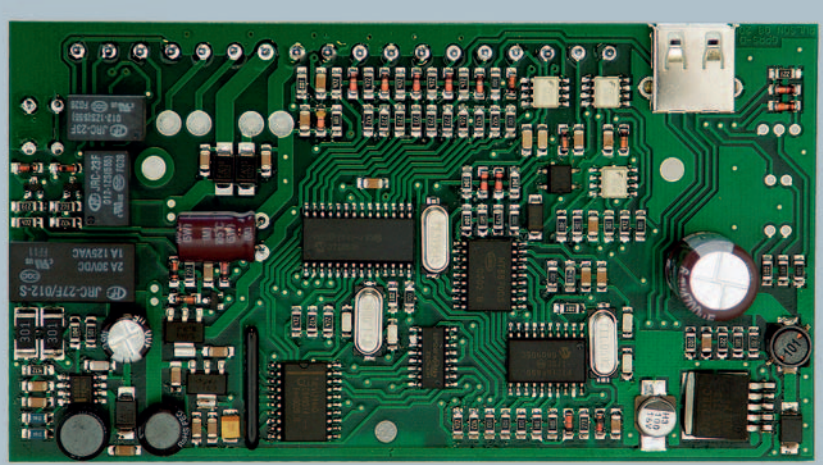
GPRS-D został tak zaprojektowany, by umożliwić centrali alarmowej transmisję sygnałów za pośrednictwem podłączonej do układu linii telefonicznej. Jeśli linia jest sprawna, jest stale podłączona do zacisków centrali alarmowej. Zgodnie z normami dla urządzeń telefonicznych, układ detekcji stanu linii telefonicznej oparty jest na pomiarze prądu w linii, a symulator linii wytwarza napięcie -25 V względem masy. Zastosowane rozwiązania układowe sprawiają, iż jest to prawdopodobnie jedyny na rynku tego typu nadajnik, zapewniający poprawną współpracę z większością central alarmowych.

W przypadku wystąpienia zdarzenia alarmowego centrala rozpoczyna procedurę łączenia ze stacją monitorowania. Odbiornik DTMF analizuje, jaki numer wybiera, i jeśli jest on zgodny z zaprogramowanym w nadajniku, układ przełącza zaciski centrali do symulatora linii. Od tego momentu dialer centrali komunikuje się z odbiornikiem DTMF modułu GPRS-D podobnie jak ze stacją odbiorczą monitorowania telefonicznego. Jeśli numer wybrany przez centralę alarmową nie zgadza się z zaprogramowanym w nadajniku, układ pozostawia linię zewnętrzną dołączoną do zacisków centrali, umożliwiając jej komunikację z odległą stacją odbiorczą. W przypadku awarii lub braku zewnętrznej linii telefonicznej centrala współpracuje tylko z symulatorem linii.

Możliwe są dwa tryby współpracy z centralą alarmową – z oczekiwaniem na potwierdzenie ze stacji odbiorczej lub bez potwierdzenia. W pierwszym przypadku nadawane przez centralę alarmową komunikaty DTMF są wysyłane do



Fot. 1. Płytka nadajnika GPRS-N – widok od strony elementów



Fot. 2. Płytka nadajnika GPRS-D – widok od strony elementów. Różnica w ilości elementów daje informację jak rozbudowany musi być układ dla poprawnej pracy z DTMF

SMSCI i po odebraniu potwierdzenia ze stacji generowany jest sygnał zakończenia transmisji dla centrali. W drugim przypadku zdarzenia z centrali są buforowane i sygnał zakończenia wysyłany jest bezpośrednio po ich odebraniu.

Inne funkcje

Nadajniki GPRS-N i GPRS-D są w trybie pracy GSM są w pełni kompatybilne z produkowanym wcześniej nadajnikiem GSM1. Podobnie jak poprzednik, mają możliwość zdalnej konfiguracji parametrów pracy. Wszystkie ustawienia mogą być modyfikowane lokalnie, poprzez podłączenie do komputera z zainstalowanym dedykowanym oprogramowaniem.

Urządzenia, pracując w trybie GPRS, zyskują nowe możliwości kontroli łączności ze stacją SMSCI. Podobnie jak w nadajniku GSM1, możliwe jest zaprogramowanie wysyłania testu okresowego z obiektu. Kod testu jest dwuznakowy i może być programowany przez operatora (kod testu okresowego GPRS jest taki sam, jak kod testu w trybie GSM). Okres testów może być ustawiony w zakresie 15 minut – 24 godziny. Testy okresowe wymagają potwierdzenia ze strony stacji odbiorczej – brak potwierdzenia w trybie GPRS spowoduje przełączenie nadajnika do trybu GSM i powtórne wysłanie testu w postaci SMS.

Poza testami okresowymi w trybie GPRS moduł nadawczy wysyła sygnały kontrolne TN (testy niejawne) z wybranym przez użytkownika okresem 10 s, 30 s lub 60 s (zgodnie z normą PN-EN50136-1-1:2007). Testy niejawne nie wymagają potwierdzeń ze strony stacji odbiorczej. Ze względu na ograniczone możliwości przetwarzania danych przez programy archiwizacji zdarzeń, analiza i sygnalizacja braku testów niejawnych realizowana jest bezpośrednio w stacji odbiorczej SMSCI. Brak trzech kolejnych sygnałów z obiektu powoduje wygenerowanie przez stację SMSCI zdarzenia o kodzie BT z numerem danego obiektu. Powrót testów niejawnych sygnalizowany jest kodem NN (taki sam kod zostanie wygenerowany przez stację w momencie zarejestrowania pierwszego testu niejawnego z obiektu, czyli włączenia do sieci nowego nadajnika).

Możliwe jest wyłączenie wysyłania TN i wówczas kontrola łączności, podobnie jak w systemie GSM, realizowana jest na poziomie oprogramowania archiwizującego, poprzez analizę braku potwierdzanych testów okresowych.

Podsumowanie

Kontrola łączności wykorzystująca ramki TN realizowana w stacji SMSCI pozwala znacznie zwiększyć częstotliwość sygnałów kontrolnych wysyłanych przez nadajniki, bez obciążania łącza pomiędzy stacją odbiorczą i komputerową bazą obiektów.

Pakietowa transmisja danych GPRS, zastosowana w systemach bezprzewodowego nadzoru obiektów monitorowanych, obniża koszty usługi w stosunku do aplikacji opartych na komunikacji SMS. **Jednocześnie traktowanie łączności SMS jako uzupełnienia systemu transmisji GPRS zwiększa niezawodność systemu**.

Komunikacja z centralami alarmowymi w standardzie Contact ID stwarza możliwości precyzyjnego lokalizowania i interpretacji zdarzeń w monitorowanych obiektach bez udziału telefonicznych linii komutowanych.

Opisane urządzenia są przykładem profesjonalnego wykorzystania nowoczesnej technologii w dziedzinie monitorowania i bezprzewodowego powiadamiania o zdarzeniach w obiektach chronionych, a ich wdrażanie jest istotnym krokiem w rozwoju agencji ochrony mienia.

Rafał Miklaszewski
Pulson

ul. Smoleńskiego 2, 01-698 Warszawa
tel: 022 639-34-36, fax: 022 833-48-60
e-mail: visonic@visonic.com.pl
www.visonic.com.pl

Visonic®
For a secure way of life

Designed by Linor Ankri

PowerMaxPro

Bezpieczny styl życia z nowoczesnym systemem

DWUKIERUNKOWY PILOT LCD

CZUJNIK Z OPTYKĄ LUSTRZANĄ

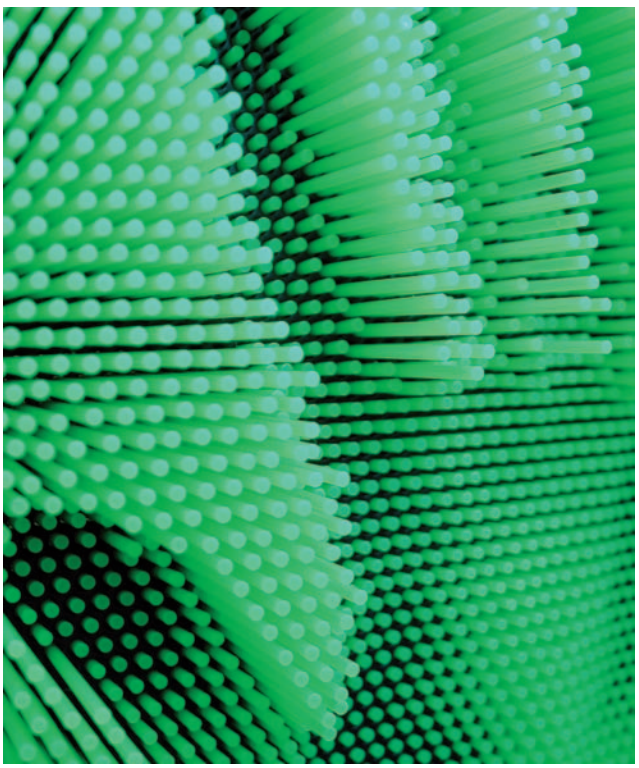
BEZPRZEWODOWY SYGNALIZATOR ZEWNĘTRZNY

- Bezprzewodowa komunikacja dwukierunkowa
- Nowoczesny, elegancki wygląd
- Prosta obsługa
- Szybka instalacja
- Certyfikat TECHOM - klasa C

Alpol: Warszawa Mokotów 032 790 76 34 Warszawa Praga 032 790 76 33 Katowice 032 790 76 56 Kraków 012 415 13 51 Łódź 032 790 76 25 Wrocław 032 790 76 27 Poznań 032 790 76 37 Szczecin 032 790 76 30 Bielsko-Biała 032 790 76 21 Gliwice 032 790 76 23 Lublin 032 790 76 50 Sopot 032 790 76 43 **ASD Systemy Zabezpieczeń**: Łódź 042 656 43 05 **Elektron**: Kraków 012 416 19 11 **Interfach 2**: Radom 048 34 00 600 **Patronic** Szczecin: 091 48 41 241 Gorzów Wielkopolski: 095 720 67 34 Zielona Góra: 068 32 56 399 Jelenia Góra: 075 644 09 97 **Proxima Alarm Group**: Toruń 056 661 18 96 **Solar Polska**: Łódź: 042 677 58 00 Kraków: 012 638 91 00 Lublin: 081 745 59 00 Poznań: 061 863 02 04 Szczecin: 091 485 44 00 Wrocław: 071 377 19 00 **S.P.S. Trading**: Warszawa: 022 518 31 50 Łódź 042 617 00 32 Wrocław 071 348 44 64 Poznań 61 852 19 02 **Supervision** Oleśnica: 071 787 30 16

Nie bójmy się biometrii!

Publikując w ostatnim roku kilka artykułów dotyczących biometrii, żywiliśmy nadzieję, że również przy naszym skromnym udziale w mnogości artykułów dotyczących systemów automatycznej identyfikacji uda się choć w niewielkim stopniu wzbudzić społeczne poczucie swoistego oswojenia z technologią biometryczną. Naszą ideą było zaszczepienie zainteresowania a tym samym i chęci głębszego zrozumienia tej technologii. Oczywiście zdawaliśmy sobie sprawę z tego, że przedstawiając, oprócz zalet, również aspekty mogące budzić niepokój, nie ułatwiamy ekspansji rynku biometrycznego w polskich warunkach, lecz w większym stopniu braliśmy pod uwagę wagę obiektywizmu w prezentowaniu wiedzy i fakt, że pomimo społecznych obaw dotyczących biometrii jej akceptacja i implementacja w systemach bezpieczeństwa jest nieunikniona, co wynika z rozwoju cywilizacyjnego.



Artykuł ten będzie próbą uzmysłowienia rosnącej konieczności wdrażania systemów automatycznej identyfikacji wykorzystujących technologię biometryczną oraz odniesienia się do aspektów prawnych, które w obecnej formie niejednokrotnie stają się dobrą wymówką, tłumaczącą sprzeciw wobec biometrii (co nie ma odzwierciedlenia w rzeczywistości prawnej). Niejednokrotnie spotykamy się z tendencją do ostrego sprzeciwu wobec biometrii, ze strachem przed stworzeniem reżimu pracy (poprzez rejestrację czasu pracy) oraz wyszukiwaniem legislacyjnych argumentów świadczących o sprzeciwie wobec biometrii bądź też nakładających na pracodawców dodatkowe zobowiązania legislacyjne. Świadczyć to może o braku znajomości zagadnień biometrii, a także strachu przed ograniczeniem zakorzenionej w nas tendencji do kombinowania oraz swobodnego traktowania przepisów i regulaminów.

Zagadnienia te są obecnie w Polsce niezwykle żywe i ważne, dlatego też przytoczymy w niniejszym artykule wnioski, jakie nasunęły się nam podczas realizacji badania pt. *Biometria w systemie bezpieczeństwa człowieka – moda czy konieczność?,* przeprowadzonego na początku 2007 r. W badaniu tym, oprócz własnych analiz dotyczących pięciu hipotez roboczych, dokonaliśmy porównania naszych wyników z wynikami ankiet przeprowadzonych w 2005 r. m.in. przez TNS (TNS Canadian Facto – dla Kanady, TNS NFO – dla USA) i TRUSTe, odnoszących się do stosunku obywateli wobec wykorzystania biometrii w personalnych dokumentach tożsamości.

Badanie „Biometria w systemie bezpieczeństwa człowieka – moda czy konieczność?"

Dla wyjaśnienia tematu naszych badań na początek zdefiniujemy pojęcia „mody" i „konieczności" w odniesieniu do biometrii, które zostały zawarte w tytule badania.

Zatem *moda* (łac.) to pojęcie socjologiczne, oznaczające powszechnie przyjęty zwyczaj (dotyczący głównie rzeczy zewnętrznych, widocznych, zwłaszcza stylu, sposobu ubierania się, zachowywania), ulegający częstym zmianom. Moda przejawia się w szerokim zakresie rzeczy i zachowań należących do kultury, do sposobu życia danej grupy ludzi. Wynika z potrzeby naśladowania innych, identyfikowania się z nimi. Ta psychiczna potrzeba jest najwyraźniej widoczna w ubiorze, wizerunku, ale moda występuje także w innych dziedzinach życia społecznego. Moda na biometrię to moda na nowoczesność (nowinki technologiczne, bezpieczeństwo), która może być wyrazem naśladownictwa interesujemy się nowościami, z których korzystają już inni), poczucia wyższości związanego z uczestnictwem w postępie. Ignorowanie mody czy sprzeciw wobec niej może narazić człowieka lub instytucję na zarzut staromodności (a więc nienadążania za postępem), zwykle odczuwany jako lekceważący czy ośmie-

szający. Moda może być traktowana jako teren rywalizacji między ludźmi lub instytucjami, której celem jest osiągnięcie przewagi nad rywalem. Może to nawet prowadzić do swoistego przymusu mody – lekceważenie jej grozi izolacją, ostracyzmem, wyalienowaniem lub po prostu wypadnięciem z rynku. Nadążanie za modą może być formą reklamy, prezentującą naszą firmę jako w pełni profesjonalną i ekskluzywną, o wysokim prestiżu i budzącą zaufanie. Moda na biometrię w naszym kraju będzie zapewne wynikiem przyjętych już i mocno akcentowanych w krajach rozwiniętych standardów bezpieczeństwa oraz identyfikacji osób, niejednokrotnie zaczerpniętych choćby z filmów, takich jak np. 2001: *Odyseja Kosmiczna* (1968 rok – głos), *GoldenEye* (1995 rok – głos, dłoń, tęczówka), *Ultraviolet* (2006 rok – DNA, głos, tęczówka, twarz i struktura czaszki, fizjologiczna budowa głowy, struktura skóry, puls, oddech, analiza poligraficzna), *Raport mniejszości* (2002 rok – ogólna wizja przyszłości). Oczywiście w niektórych przypadkach sposób działania biometrii jest przedstawiony wysoce przesadnie (np. skanowanie tęczówki oka laserem podczas jej identyfikacji; posłużenie się wyrwaną gałką oczną do oszukania systemu biometrycznego). Zdarza się, że film przedstawia technologie jeszcze wciąż futurystyczne, ale zarazem wyznacza kierunek poszukiwań. Wyżej wymieniona analiza poligraficzna już dziś funkcjonuje w wydaniu gotowego systemu Cogito 1002, o którym pisaliśmy na łamach niniejszego czasopisma. Od 2003 r. na amerykańskich lotniskach funkcjonuje system obserwacji mimiki podróżnych, w którym wyspecjalizowane patrole kwalifikują podejrzanych osobników do dokładnego sprawdzenia. Do 2012 r. ma on zostać w pełni zautomatyzowany poprzez wykorzystanie nowoczesnych kamer, laserowego śledzenia ruchu gałki ocznej, mikrofonów oraz czujników częstotliwości uderzeń serca i szybkości oddechu.

Paradoksalnie moda na stosowanie biometrii może mieć charakter ambiwalentny. Z jednej strony może zwiększyć nasze bezpieczeństwo i uczynić przyjemnym współczesny natłok haseł i PIN-ów, kodów dostępu i permanentnych kontroli w bankach, sądach, portach lotniczych i morskich, z drugiej zaś strony może stanowić zagrożenie dla moralności, ułatwiając instytucjom państwowym ingerencję w życie prywatne obywateli, śledzenie i manipulację, czyli zachowania dotychczas uznawane za niemoralne, a w dalszej konsekwencji kreowanie sytuacji politycznej.

Pojawiające się w temacie badań słowo „konieczność" oznacza właściwość układu zjawisk lub aspekt związku przyczynowego określany jako: „to, co nie może nie być (nie zachodzić)" lub „to, co nie może zachodzić inaczej niż zachodzi". W odniesieniu do naszego badania oznacza to, że biometria nie może nie być zauważona i nie zostać wykorzystana jako niezwykle istotny element składowy systemów bezpieczeństwa (w dobie społeczeństw informacyjnych), jednoznacznie identyfikujący osobniki uczestniczące w procesach systemu. Trzeba przy tym uznać za bezsporny fakt, że jak dotychczas najsłabszym ogniwem systemów bezpieczeństwa jest człowiek.

Odpowiednio wykorzystana biometria może ustanowić przełom w dziedzinie bezpieczeństwa, a zatem sama w sobie będzie koniecznością, której zaprzeczanie pozostawi nas na marginesie życia społecznego.

Hipotezy badawcze i ich weryfikacja

Na początku roku, prowadząc własne badanie, poruszaliśmy się wokół kilku hipotez roboczych. Poniżej zaprezentujemy je i przedstawimy ich weryfikację, uwzględniając wszystkie przeanalizowane przez nas ankiety.

Pierwsza postawiona przez nas hipoteza była odpowiedzią na pytanie o to, czy współczesne społeczeństwa w obliczu nowych zagrożeń oczekują przełomu w dziedzinie bezpieczeństwa, i brzmiała: *Zagrożenia nowego świata wyszły poza granice dotychczas stosowanych mechanizmów zapobiegania im oraz ich neutralizacji. Początek zmian jest związany z wydarzeniami z 11 września 2001 r. Społeczeństwa w obliczu zagrożenia terroryzmem wykorzystującym zdobycze współczesności oczekują przełomu (nowego narzędzia i mechanizmu), by poczuć się bezpiecznie.*

Ponad połowa (52%) naszych ankietowanych opowiada się przeciw potrzebie dokonania jakiejkolwiek rewolucji w zakresie zapewniania bezpieczeństwa, a 72% respondentów ma poczucie pełnego bezpieczeństwa. Z kolei aż 48% badanych jest za przełomem w tym zakresie, a 78% badanych zapytanych o to, czy potrzeba bezpieczeństwa jest dziś tylko sztucznie wykreowana przez media, zgodziło się, że ta potrzeba jest rzeczywista, a więc musi mieć swoje źródło w realnych zagrożeniach dotykających nas bezpośrednio i pośrednio (ataki terrorystyczne w USA, Hiszpanii, Anglii, Iraku). 54% respondentów uważa nowoczesne technologie (zdobycze współczesności) za broń używaną również przez terrorystów i pospolitych przestępców, wykorzystywaną przeciwko nam. Wynika z tego, że rozwój cywilizacji niesie ze sobą niebezpieczeństwa i powoduje, że zabezpieczenia wciąż są w tyle za narzędziami ataku, a więc że postęp to źródło nowych niebezpieczeństw. Obecnie zdajemy sobie sprawę z zagrożeń i ich genezy, lecz dopóki nie dotykają nas one osobiście i nie czujemy strachu z powodu ich bliskości, mamy poczucie pełnego bezpieczeństwa. Wziąwszy pod uwagę wyżej wymienione odpowiedzi, trudno jest uznać przyjętą hipotezę za zweryfikowaną, choć w odpowiedzi na bezpośrednie pytanie respondenci uznali jej słuszność. Należałoby uszczegółowić pytania dotyczące tego problemu badawczego bądź też inaczej je sformułować.

Kolejna nasza hipoteza była związana z pytaniem o to, czy biometria jest wysoce wiarygodnym sposobem uwierzytelniania tożsamości i czy w świadomości społecznej ma ona duże znaczenie w systemach bezpieczeństwa. Brzmiała ona: *Wykorzystanie biometrii w dobie społeczeństw informacji jest jedynym dobrym sposobem uwierzytelniania (kontroli tożsamości), który może zostać z powodzeniem wykorzystany w systemach bezpieczeństwa.*

Aż 84% ankietowanych uznało biometrię za wysoce wiarygodny sposób potwierdzania tożsamości. 72% ankietowanych wierzy w skuteczność biometrii w walce z kradzieżami tożsamości. 53% chce wykorzystania biometrii w walce z terroryzmem (biometryczna kontrola tożsamości), a 45% respondentów uważa dokumenty biometryczne za ważny element bezpieczeństwa. Wyniki badań prowadzonych w innych krajach również świadczą na rzecz przyjmowanej przez

nas hipotezy. Bardzo wielu ankietowanych (74% Kanadyjczyków i 69% Amerykanów) uważa, że biometria w sposób znaczący ograniczy kradzieże tożsamości oraz swobodę działania terrorystów (58% ankietowanych Kanadyjczyków i 51% Amerykanów). Jest jeszcze jedna interesująca kwestia. Nasi respondenci są w opozycji do badanych przez TNS i aż 58% podpisuje się pod stwierdzeniem „nie ufam technologii biometrycznej", natomiast ankietowani w Kanadzie (40%) i USA (46%) nie zgadzają się z tym stwierdzeniem – za jest zaledwie 19%. Z kolei wszyscy ankietowani są zgodni co do tego, że przestępcy znajdą sposób na obejście lub złamanie zabezpieczeń biometrycznych.

Następna nasza hipoteza miała związek z pytaniem o to, czy całe społeczeństwo jest przygotowane na szybkie tempo wdrażania nowinek technologicznych i proceduralnych, na swoistą rewolucję związaną z wprowadzaniem wszechobecnych systemów biometrycznych, i brzmiała: *Istnieje duże zróżnicowanie co do wiedzy i akceptacji czy też zrozumienia nowych technologii, w tym biometrii. Samo społeczeństwo informacyjne wprowadza wiele niejednorodności w swą strukturę, czyniąc wielu członków społeczeństwa wyalienowanymi właśnie z powodu nienadążania za rozwojem.*

Tej hipotezy nie udało się zweryfikować w sposób bezpośredni. Sugerujemy, że należałoby rozszerzyć grupę ankietowanych poza środowisko akademickie. Na podstawie własnych obserwacji i doświadczeń sądzimy, że stosunek do nowoczesności bywa różny. Jednych fascynuje nowość i dlatego chętnie sięgają po nowinki. Dotyczy to przeważnie młodych ludzi. Inni, np. ludzie starsi, boją się nowoczesności – niektórzy panicznie. Z informacji zawartych w przeprowadzonym przez nas wywiadzie swobodnym wynika, że różne środowiska są niechętne wobec biometrii (wyraża się to m.in. w „sabotowaniu" czytników biometrycznych, składaniu skarg do GIODO, niewyrażaniu zgody na korzystanie z czytników biometrycznych). Wydaje się zatem, że nie wszyscy są przygotowani na szybkie tempo wdrażania nowinek technologicznych.

Za potwierdzeniem hipotezy może przemawiać rozbieżność w odpowiedziach udzielanych przez ankietowanych, wynikająca prawdopodobnie z niezrozumienia technologii biometrycznych. Z jednej strony biometria uważana jest za element, który zwiększy bezpieczeństwo, z drugiej – za coś, co może być wykorzystane przeciwko nam. Biometria ograniczy kradzieże tożsamości i swobodę działania terrorystów, ale przestępcy znajdą sposób na obejście tej technologii. Ta ambiwalencja może mieć pewne uzasadnienie w samej technologii, ale wśród ankietowanych wynika raczej z jej nieznajomości i niezrozumienia.

Hipotezę stanowiącą odpowiedź na pytanie, czy i w jakim stopniu społeczeństwo obawia się ograniczenia swobód i poczucia wolności na rzecz bezpieczeństwa, sformułowaliśmy następująco: *Istnieje duża obawa społeczna co do ograniczenia swobód poprzez wprowadzenie biometrycznych systemów kontroli tożsamości.*

Hipoteza ta została w pełni potwierdzona. 58% ankietowanych wyraża przekonanie, że biometria przyczyni się do ograniczenia swobód i wolności obywateli, a 36% ankietowanych nie umiało zająć stanowiska. W ankiecie TNS/e-TRUST aż 61% ankietowanych (przy 28% respondentów nie mających zdania) uważa, że biometria ograniczy swobodę i prywatność oraz posłuży jako marker obywateli w celach inwigilacji. 61% badanych mieszkańców USA i 61% Kanadyjczyków oraz 58% naszych badanych uważa, że istnieje duże prawdopodobieństwo niewłaściwego użycia danych biometrycznych przez administrację rządową. Jest to trudna kwestia do rozstrzygnięcia.

Ostatnia postawiona przez nas hipoteza, związana z pytaniem, czy słuszne jest, zwłaszcza dziś, tak silne akcentowanie problemu bezpieczeństwa, została sformułowana jako maksyma i brzmiała następująco: *Bezpieczeństwo nie jest wszystkim, ale wszystko bez bezpieczeństwa jest niczym.*

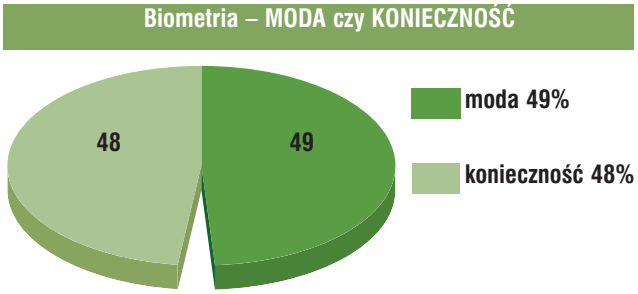
Hipoteza ta wydaje się słuszna, mimo że nie została zweryfikowana w sposób bezpośredni – analiza zebranych materiałów potwierdziła ją pośrednio. We współczesnym, pełnym zagrożeń świecie bezpieczeństwo nabiera nowego znaczenia i to ono nadaje sens wszelkiej ludzkiej działalności.

Podsumowanie badań i wnioski

Na podstawie przeprowadzonych badań sformułowaliśmy następujące wnioski:

1. Ankietowani mają poczucie pełnego bezpieczeństwa.
2. Silne akcentowanie i poruszanie problemu bezpieczeństwa jest słuszne.
3. Potrzeba większego bezpieczeństwa istnieje w krajach, w których miały miejsce ataki terrorystyczne.
4. Nie jest wyraźnie rozstrzygnięta kwestia zapotrzebowania na rewolucję w sposobach zapewniania bezpieczeństwa. Za rewolucją jest 52% ankietowanych, przeciw – 48%. Może to oznaczać wymaganie nadmiarowości w bezpieczeństwie (jest bezpiecznie, ale może będzie jeszcze bezpieczniej) bądź też odniesienie do ataków w innych krajach, w których złamano zabezpieczenia.
5. Istnieje przekonanie, że nauka służy bardziej powstawaniu zagrożeń i atakom skierowanym przeciwko nam (łamaniu zabezpieczeń) niż budowaniu bezpieczeństwa.
6. Pojęcie biometrii jest powszechnie znane, lecz tylko w dość ogólnym ujęciu.
7. Istnieje poparcie dla powszechności biometrii, lecz tylko w aspekcie bezpieczeństwa narodowego (potrzeba biometrycznego paszportu i dowodu osobistego, akceptacja wykorzystania biometrii na przejściach granicznych, lotniskach i w metrze).
8. Największe zaufanie wzbudza technologia odcisku palca i rozpoznawania tęczówki oka.
9. Istnieje wyraźna obawa, zarówno społeczna jak i instytucjonalna, wobec nieuzasadnionego użycia biometrii.
10. Istnieje obawa, że biometria umożliwi ograniczenie swobód i wolności obywateli.
11. Istnieje obawa przed możliwością obejścia/złamania biometrycznych zabezpieczeń.
12. Istnieje przekonanie, że biometria ograniczy w sposób zasadniczy kradzieże tożsamości i działania terrorystów.
13. Ankietowani na terenie Wojskowej Akademii Technicznej nie mają zaufania do technologii biometrycznej. Zaufanie do biometrii mają ankietowani z USA i Kanady.
14. Istnieje przekonanie, że biometria daje wygodę i zaawansowaną funkcjonalność.
15. Wprowadzanie biometrii w systemach bezpieczeństwa to **konieczność**, ale także **moda**.

Biometria (ze wszystkimi zaletami i wadami) jest dziś koniecznością. W różnych środowiskach jest różnorodnie oceniana. Obecnie jest również modna, ponieważ jest czymś nowoczesnym. Może z tego powodu stanowić dobrą reklamę instytucji lub firmy. Chociaż wciąż napotykamy niepełne zrozumienie biometrii lub niechęć do niej, rozszerzająca się moda może to zmienić i spowodować jej akceptację, a co za tym idzie – wdrażanie jej na szeroką skalę w systemach bezpieczeństwa

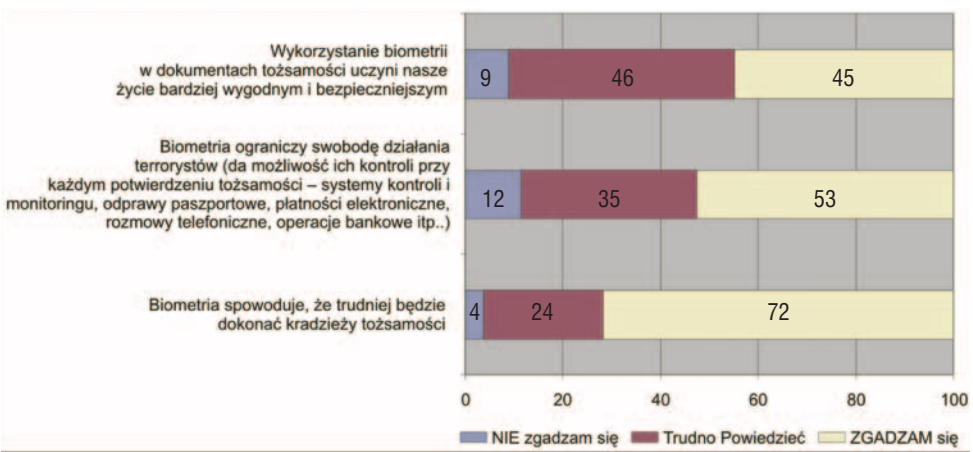


Biometria w Polsce

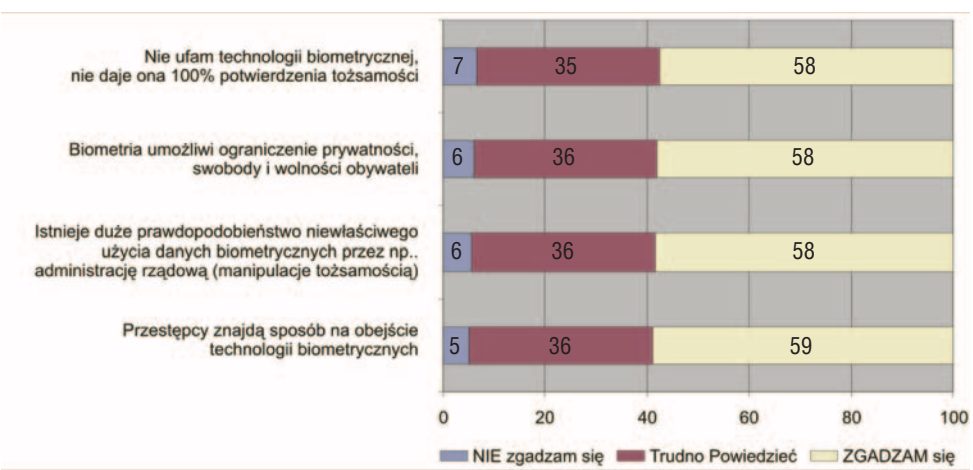
Motorem zmian w naszym kraju może okazać się organizacja Euro 2012. Wymagania odnośnie bezpieczeństwa imprez masowych mogą wymusić konieczność instalacji systemów biometrycznych w rozległych obiektach użyteczności publicznej (na stadionach, na lotniskach, w metrze) oraz wprowadzenie biometrycznego dowodu osobistego.

W Polsce rynek biometryczny wciąż rozwija się mało dynamicznie. Obawy i uprzedzenia wpływają negatywnie na chęć rozwijania i stosowania technologii biometrycznych. Niektórzy uważają, że technologie biometryczne mogą spowodować fizyczną szkodę, uszczerbek na zdrowiu albo że użycie skanerów biometrycznych jest niehigieniczne (przenoszenie chorób poprzez kontakt fizyczny). **Ale czy zastanawiamy się nad tym, ile razy każdego dnia dotykamy np. banknotów, które odwiedzają niemalże wszystkie portfele?** Obawiamy się, że nasze personalia, ujawniane dzięki biometrycznym metodom, mogą być niewłaściwie wykorzystane (fałszowanie danych, manipulowanie nimi, sprzedaż danych biometrycznych przez przestępców, pozostawianie na miejscu przestępstwa cudzych danych biometrycznych). **Ale czy zastanawiamy się nad tym, ile informacji o nas można zdobyć na podstawie białego wywiadu (informacje te są niemal powszechnie dostępne dla każdego)?**

Wydaje się, że każdy system można próbować skompromitować. Potrzeba tylko czasu, pieniędzy i odpowiedniej technologii. Przykładem może być paszport biometryczny – opracowano go niedawno, a już teraz niemieccy „specjaliści" donoszą, że udało im się w warunkach laboratoryjnych dokonać zdalnego odczytu zawartości mikroprocesora. Wypada zapytać, co może zdarzyć się w przeciągu dziesięciu lat, w okresie ważności paszportu. Takie pytania należy zadawać – nie po to, by podważać sens technologii, lecz by zapobiegać nieprawidłowościom. To przeciwdziałanie z kolei wprowadza nas w błędne koło, które jest jak gonitwa psa za własnym ogonem. Kto wśród specjalistów bezpieczeństwa oraz atakujących jest psem, a kto ogonem pozostawiamy bez wskazania. To błędne koło dodatkowo zmusza nas do „ograniczania przestrzeni życiowej" poprzez ograniczenia swobody i intymności. Już teraz doświadczamy rozdźwięku pomiędzy ograniczeniem wolności a wzrostem poczucia bezpieczeństwa. Międzynarodowy zespół neurologów opracował technologię umożliwiającą analizowanie naszych fal mózgowych i określanie w ten sposób, o czym myślimy. Czy jest to urzeczywistnienie idei z opowiadania Philipa K. Dicka *Minority Report*, zekranizowanego przez Stevena Spielberga? Prof. Colin Blakemore, brytyjski neurobiolog, dyrektor British Medical Research Council

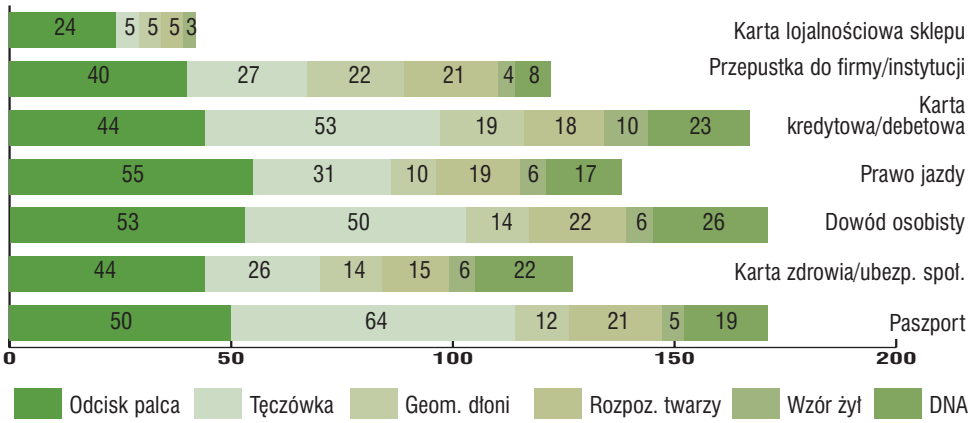


Zdecydowana większość ankietowanych (72%) uważa, że biometria znacznie ograniczy kradzieże tożsamości i przestępstwa z tym związane. 53% uważa także, że ograniczy swobodę działania terrorystom. Z kolei tylko 45% ankietowanych podpisało się pod stwierdzeniem, że biometryczne dokumenty tożsamości zapewnią nam wygodę i bezpieczeństwo.



Ponad połowa ankietowanych nie ufa technologii biometrycznej i wyraża przekonanie, że umożliwi ona ograniczenie naszej prywatności, że może być ona wykorzystana przeciwko nam przez administrację mającą dostęp do bazy danych biometrycznych oraz że przestępcy i tak znajdą sposób na obejście zabezpieczeń biometrycznych.

(MRC), uważa, że wykrywanie przestępstw, które dopiero mogą zostać popełnione, jest tylko kwestią czasu. Gdzie jest zatem granica naszej prywatności? Czy jesteśmy w stanie zaakceptować tak dalece posunięte technologie? Nie znamy odpowiedzi na te pytania. Można je odrzucić, zamiast szukać odpowiedzi, ale jest to równoznaczne z odrzuceniem idei nowoczesnego społeczeństwa.



Największym poparciem cieszy się technologia rozpoznawania odcisku palca. Dotyczy to wszystkich wymienionych typów dokumentów. W przypadku paszportu i kart kredytowych większe poparcie uzyskała technologia tęczówki oka.

Barierą w ekspansji biometrii mogą być ograniczenia wynikające z braku odpowiednich uregulowań prawnych (przepisów prawa administracyjnego i cywilnego) bądź też niejednoznaczna interpretacja już istniejących przepisów i niedostosowanie ich do rozwijających się technologii.

Najwięcej emocji budzi kwestia samych danych biometrycznych – informacji o unikatowych genotypowych i fenotypowych cechach osoby, umożliwiających jej automatyczne uwierzytelnienie. Zgodnie z definicją danych osobo-

wych, zawartą w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, wszelkie dane biometryczne są danymi osobowymi. Stosowanie biometrii musi zatem być zgodne z ustawą o ochronie danych osobowych, która normuje ochronę danych osobowych w sposób całościowy, odnosząc się do różnych dziedzin prawa, a jej adresatami pozostają zarówno podmioty sektora publicznego jak i prywatnego, o ile decydują o celach i środkach przetwarzania danych osobowych.

Informacje o cechach biometrycznych określone w ustawie mają w zasadzie charakter danych zwykłych, choć niektóre z nich (np. dane o sposobie chodzenia, pisania ręcznego, unikatowe dane z charakterystyki EEG) mogą być uznane za informacje o stanie zdrowia, a więc za dane wrażliwe, których przetwarzanie jest zabronione. Dane wrażliwe zostały przez ustawę jednoznacznie określone, są to dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanie zdrowia, kodzie genetycznym (biometryczne rozpoznawanie z wykorzystaniem DNA), nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu, mandatów karnych i innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Nie bez kozery przytaczamy tu tę wyliczankę informacji wrażliwych, których ujawnienie jest aktem godzącym w naszą prywatność i intymność. Cecha biometryczna to ta, która „zaledwie" albo „aż" identyfikuje tożsamość, nie dając przeciw nam broni, jaką może być portret psychologiczny (zachowań, przyzwyczajeń, chorób) stworzony na podstawie danych wrażliwych. Piszemy o tym po to, aby pokazać, że biometria nie narusza naszej prywatności i intymności życia osobistego.

Z zapisów ustawy o ochronie danych osobowych wynikają administracyjno-prawne ograniczenia przetwarzania biometrycznych danych osobowych. Przetwarzanie ich jest uwarunkowane:

- istnieniem podstawy legalizującej,
- zapewnieniem bezpieczeństwa danych,
- uwzględnieniem uprawnień osób, których dane są przetwarzane,
- podleganiem kontroli Generalnego Inspektora Ochrony Danych Osobowych,
- zgłoszeniem zbioru danych do rejestracji.

Zgodnie z ustawą z dnia 13 lipca 2006 r. o dokumentach paszportowych (biometrycznych) w dniu 28 sierpnia 2006 r. powstała centralna ewidencja, która stanowi zbiory danych (biometrycznych) zgromadzonych w ewidencjach paszportowych. Dane przetwarzane w centralnej ewidencji paszportowej udostępnia się w zakresie niezbędnym do wykonywania ustawowych zadań Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, ministrowi odpowiedzialnemu za finanse publiczne, policji, prokuratorowi, sądowi, służbie więziennej, służbie kontrwywiadu wojskowego, służbie wywiadu wojskowego, żandarmerii wojskowej.

Dane z centralnej ewidencji mogą być udostępniane na podstawie umów międzynarodowych, których stroną jest Rzeczpospolita Polska.

Wziąwszy pod uwagę liczbę wyżej wymienionych instytucji oraz fakt, że najsłabszym ogniwem systemów bezpieczeństwa jest człowiek, można dojść do przekonania, że nasze

dane biometryczne (wzorce biometryczne) nie są całkiem bezpieczne, nawet przy zachowaniu wymogów ustawy.

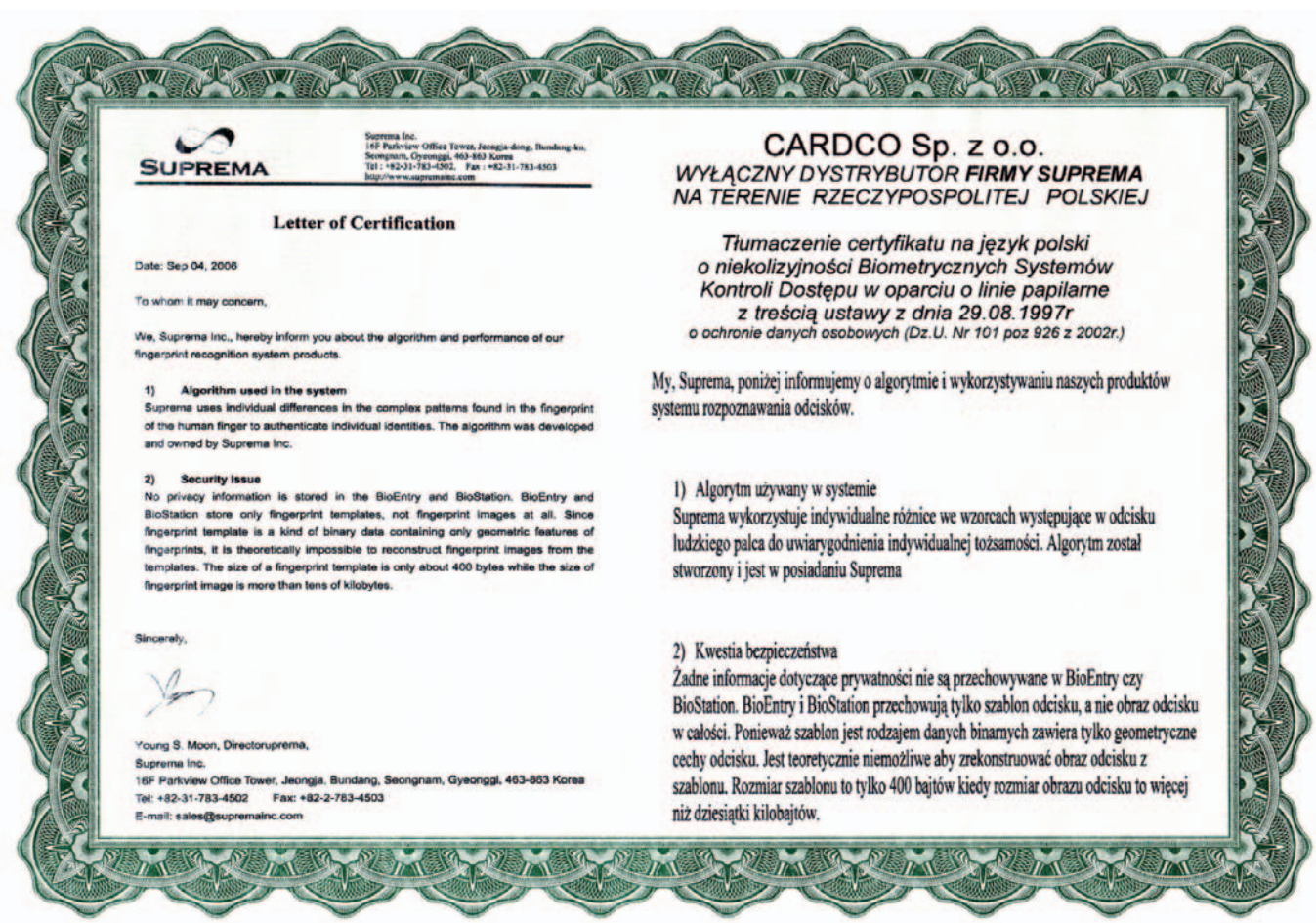
By zwiększyć bezpieczeństwo systemów biometrycznych, a tym samym uniknąć kradzieży wzorca, można zastosować różne metody. Można przechowywać wzorzec na karcie mikroprocesorowej, służącej do uwierzytelniania tożsamości użytkownika. Można także, po dokonaniu ekstrakcji unikatowej cechy charakteryzującej tożsamość, wzoru biometrycznego, wybrać niezbędną liczbę charakterystycznych punktów (tzw. szablon) takiego wzoru, określonych algorytmem producenta, i uzyskać tym samym wartość binarną (identyfikator – w zasadzie funkcjonalnie tożsamy np. z PIN) przechowywaną w czytniku. Teoretycznie i praktycznie nie ma możliwości odtworzenia wzorca biometrycznego na podstawie tej wartości liczbowej, a więc wszędzie poza środowiskiem konkretnego czytnika biometrycznego wiedza o identyfikatorze jest tylko nic nie znaczącą wartością binarną i nie można zidentyfikować tożsamości osoby.

Żeby przekonać niedowiarków zasłaniających się ustawą o ochronie danych osobowych, można pokusić się w tym przypadku o stwierdzenie, iż ewentualne określenie tożsamości osoby na podstawie tej wartości binarnej wymagałoby co najmniej nadmiernych kosztów, czasu i działań, a więc w świetle ustawy nie stanowi ona danych osobowych.

Wciąż nie rozumiemy wymogów bezpieczeństwa i jesteśmy w stanie zaakceptować system kontroli dostępu wykorzystujący karty elektroniczne, którego oszukanie nie stanowi dużego wyzwania. Korzystając z przepustki samochodowej (karty elektronicznej), której powinien odpowiadać określony pojazd, możemy wjechać innym samochodem. Ktoś inny może skorzystać z naszej przepustki osobowej. Wyobraźmy sobie, jakie larum podniosłoby się, gdybyśmy musieli identyfikować swoje samochody za pomocą systemów automatycznej weryfikacji numerów rejestracyjnych bądź systemów RFID, już powszechnie stosowanych w wielu krajach.

Łatwo przyzwyczajamy się do tego, że w systemach kontroli dostępu nie wszyscy pracownicy objęci są procedurami kontroli (np. dyrektorzy firm i ich goście). W jednym z warszawskich sądów widzieliśmy, jak urządzenia skanujące bagaż i osoby w poszukiwaniu niebezpiecznych narzędzi były omijane przez wielu pracowników sądu, sprzątaczki i pracowników firm budowlanych. Systemy biometrycznej identyfikacji ułatwiłyby nam życie w powodzi haseł i kodów, ale nie pozwoliłyby na omijanie systemów zabezpieczeń – być może stąd tak silny sprzeciw wobec biometrii.

Aneta Krysowaty
Ireneusz Krysowaty
Paweł Niedziejko
Instytut Inżynierii Systemów Bezpieczeństwa



SUPREMA

Suprema Inc.
16F Parkview Office Tower, Jeongja-dong, Bundang-ku, Seongnam, Gyeonggi, 463-863 Korea
Tel : +82-31-783-4502, Fax : +82-31-783-4503
http://www.supremainc.com

Letter of Certification

Date: Sep 04, 2006

To whom it may concern,

We, Suprema Inc., hereby inform you about the algorithm and performance of our fingerprint recognition system products.

1) **Algorithm used in the system**
Suprema uses individual differences in the complex patterns found in the fingerprint of the human finger to authenticate individual identities. The algorithm was developed and owned by Suprema Inc.

2) **Security issue**
No privacy information is stored in the BioEntry and BioStation. BioEntry and BioStation store only fingerprint templates, not fingerprint images at all. Since fingerprint template is a kind of binary data containing only geometric features of fingerprints, it is theoretically impossible to reconstruct fingerprint images from the templates. The size of a fingerprint template is only about 400 bytes while the size of fingerprint image is more than tens of kilobytes.

Sincerely,

Young S. Moon, Directorupremа,
Suprema Inc.
16F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Korea
Tel: +82-31-783-4502 Fax: +82-2-783-4503
E-mail: sales@supremainc.com

CARDCO Sp. z o.o.
*WYŁĄCZNY DYSTRYBUTOR **FIRMY SUPREMA***
NA TERENIE RZECZYPOSPOLITEJ POLSKIEJ

Tłumaczenie certyfikatu na język polski
o niekolizyjności Biometrycznych Systemów
Kontroli Dostępu w oparciu o linie papilarne
z treścią ustawy z dnia 29.08.1997r
o ochronie danych osobowych (Dz.U. Nr 101 poz 926 z 2002r.)

My, Suprema, poniżej informujemy o algorytmie i wykorzystywaniu naszych produktów systemu rozpoznawania odcisków.

1) Algorytm używany w systemie
Suprema wykorzystuje indywidualne różnice we wzorcach występujące w odcisku ludzkiego palca do uwiarygodnienia indywidualnej tożsamości. Algorytm został stworzony i jest w posiadaniu Suprema

2) Kwestia bezpieczeństwa
Żadne informacje dotyczące prywatności nie są przechowywane w BioEntry czy BioStation. BioEntry i BioStation przechowują tylko szablon odcisku, a nie obraz odcisku w całości. Ponieważ szablon jest rodzajem danych binarnych zawiera tylko geometryczne cechy odcisku. Jest teoretycznie niemożliwe aby zrekonstruować obraz odcisku z szablonu. Rozmiar szablonu to tylko 400 bajtów kiedy rozmiar obrazu odcisku to więcej niż dziesiątki kilobajtów.

PROTECTOR

SYSTEM DEPOZYTARIUSZY KLUCZY

PROXSAFE FLEXX

- Obudowa wykonana ze stali (opcja: szklane lub stalowe przednie drzwi)
- Panele Flexx wyposażone w gniazda kluczy i uchwyty do kluczy
- Identyfikacja klucza w otworze
- Kontrola włożenia klucza do właściwego otworu
- Pełne zabezpieczenie sabotażowe
- Możliwość instalacji od 16 do 128 kluczy w jednej obudowie
- Możliwość łączenia depozytariuszy kaskadowo
- Pełne zabezpieczenie kluczy (cylinder z blokadą)
- Terminal sterujący z polskim oprogramowaniem, wyświetlaczem LCD oraz zaimplementowanym czytnikiem 125KHz w pełni kompatybilnym z kartami/brelokami systemu kontroli dostępu SOYAL
- Praca w magistrali RS-485 oraz w sieci LAN
- Interfejs USB/RS-485(RS-485/LAN)
- Przyrząd montażowy do zarabiania kluczy
- Oprogramowanie zarządzające w języku polskim umożliwia: pełna kontrolę nad depozytariuszem, raportowanie pobieranych/zdawanych kluczy, możliwość tworzenia użytkowników, grup kluczy i użytkowników, multiklient
- Możliwość zarządzania 64 panelami FLEXX (1024 kluczy) z poziomu jednego terminala sterującego
- Sterowanie - karta, karta + pin kod, pin kod

Obudowa o wysokości *24U*
max 128 kluczy

Obudowa o wysokości *12U*
max 64 klucze

Obudowa o wysokości *6U*
max 32 klucze

NEW

GE - PROTECTOR

Urządzenie systemu zarządzania kluczy, powstałe w wyniku współpracy z firmą **GE SECURITY**

NEW

Depozytariusz składa się z:
* elektronicznego terminala sterującego drzwiami depozytariusza (opcja: drzwi stalowe z szybą lub pełne)
* specjalnych metalowych pojemników na klucze chronionych unikalnym czterocyfrowym kodem

Terminal umożliwia:
* Zarządzanie kluczami i dostępem do depozytariusza (zarządzanie 2 depozytariuszami do 60 kluczy) dla 1000 użytkowników
* Sterowanie - karta, pin kod, pin kod + karta
* Obsługę wielu formatów kart zbliżeniowych (HID, Mifare, 125 KHz itd...) poprzez dołączenie każdego rodzaju czytników z protokółem Wiegand

www.protector-polska.pl

tel: +48 (091) 431 83 10
fax: +48 (091) 431 83 11

biuro@protector-polska.pl

Dołącz do przyszłości systemów CCTV

Kamery Bosch Dinion IP

Oto Dinion IP: jedyna kamera z możliwością pracy w sieci IP oraz jakością obrazu i parametrami doskonale znanej serii Dinion.

Kamery Dinion nieprzerwanie zdobywają kolejne nagrody za niewiarygodną jakość obrazu oraz stylową, bardzo małą obudowę. Teraz kamery sieciowe Dinion mogą pracować wszędzie tam, gdzie istnieje połączenie Ethernet, przesyłając strumieniowo obraz o jakości DVD oraz obraz analogowy do dowolnej lokalizacji w sieci. Nie musisz już troszczyć się o oddzielne źródło zasilania – kamera może być zasilana wprost z sieci Ethernet zgodnej ze standardem PoE. Kamera Dinion IP wykorzystuje kompresję o niskiej przepływności MPEG4, zapewniając efektywne wykorzystanie przepustowości sieci. Kamera może również współpracować z istniejącym już systemem dozorowym bez potrzeby stosowania dodatkowych urządzeń. Zobacz naszą kamerę Dinion IP oraz najszerszą na świecie ofertę urządzeń CCTV na naszych stronach **www.boschsecurity.pl**.

BOSCH
Technologia bliżej nas

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

Metody zabezpieczania transmisji skompresowanych danych multimedialnych

Część 1. Algorytmy

Artykuł przedstawia wybrane metody ochrony transmisji mediów strumieniowych. Jest to technika polegająca na przesyłaniu skompresowanych danych multimedialnych przez sieć w postaci strumienia pakietów przetwarzanych na bieżąco w odbiorniku, tzn. nie występuje potrzeba pobrania całego pliku przed rozpoczęciem odtwarzania. Znajduje ona zastosowanie w realizacji szeregu usług: wideo na życzenie, czyli VoD (ang. *Video-On-Demand*), telewizja internetowa, wideokonferencja, telefonia internetowa VoIP, przeglądanie baz danych z obrazami medycznymi. Pierwsza część artykułu to przegląd algorytmów kryptograficznych powiązanych z kompresją danych. Najwięcej miejsca poświęcono w nim selektywnemu szyfrowaniu. W drugiej części artykułu zostaną przedstawione opisy narzędzi dostarczających usług: poufności, uwierzytelniania i integralności oraz kontroli dostępu obrazów oraz materiału wideo, a także implementacja standardów: JPEG 2000, MPEG-4 oraz niektórych algorytmów szyfrowania wideo. Tematyka artykułu jest poruszana w źródłach poświęconych bezpiecznej transmisji multimedialnej

1. Podstawowe właściwości procesów kompresji, szyfrowania oraz danych multimedialnych

Kompresja danych prowadzi do zmniejszenia objętości danych wejściowych. Z kolei szyfrowanie zapewnia ochronę danych. Jeżeli szyfrowanie jest zastosowane przed kompresją, to losowość szyfrogramu znacząco ogranicza wydajność kompresji [FuKi05]. Jeżeli szyfrowanie następuje po kompresji, pojawiają się problemy z wbudowaniem schematu szyfrowania w zintegrowany system.

Jak można przypuszczać, zastosowanie stratnej kompresji zmniejsza rozmiar danych poddawanych szyfrowaniu, więc w tym drugim przypadku proces powinien przebiegać szybciej [FuKi05]. Jednakże zaleta płynąca z ograniczenia rozmiaru tekstu jawnego jest niewielka, ponieważ czas przetwarzania danych przez algorytm kompresji jest znacznie dłuższy od czasu operowania algorytmem szyfrowania. Wydajność szyfrowania zależy silnie od zastosowanego algorytmu kompresji.

Umiejętne połączenie obydwóch procesów wykazuje szereg zalet i jest uzyskiwane drogą modyfikacji oraz optymalizacji istniejących kryptosystemów przy uwzględnieniu specyficznego formatu danych audio-wideo [FuSo04].

Bezpośrednie szyfrowanie* całego strumienia danych multimedialnych, który z reguły posiada dużą objętość, wiąże się ze sporymi nakładami czasowymi. Dodatkowo, w porównaniu z danymi w postaci tekstowej, dane audiowizualne przenoszą mniejszą ilość informacji [WuKu00, ÖzSo04]. Zawartość informacyjna jest tu bardziej rozrzedzona, nierównomiernie rozproszona i nie jest związana ze wszystkimi bitami. W przypadku deszyfrowanych danych multimedialnych dopuszczalne są również niewielkie zniekształcenia.

2. Kryteria oceny algorytmów

Podstawowymi kryteriami oceny algorytmów kryptograficznych, zawierających kroki typowe dla kompresji danych, są: stopień kompresji, błąd średniokwadratowy kompresji, rodzaj kompresji (stratna, bezstratna), poziom bezpieczeństwa, czas przetwarzania dla obydwóch kierunków przebiegu algorytmu [Wang05, ÖzSo04]. Najczęściej wykorzystuje się algorytmy stratnej kompresji (JPEG, MPEG), w których stopień kompresji jest zróżnicowany. Jednakże czasami, ze względów prawnych, pożądane jest zastosowanie algorytmu kompresji bezstratnej. Ma to miejsce w obrazowaniu medycznym.

Dokładne określenie optymalnego poziomu bezpieczeństwa jest trudne do zrealizowania. Zależy on od rodzaju zastosowania – jest niższy dla aplikacji generujących duże ilości danych multimedialnych, nie posiadających znacznej wartości, takich jak VoD. W takim przypadku stosuje się często techniki cyfrowego zarządzania prawami autorskimi (ang. *Digital Right Management* – DRM). Trudniejsza sytuacja ma miejsce w przypadku usługi wideokonferencji, w której transmitowane są, przykładowo, kluczowe firmowe uzgodnienia, a jednocześnie przepływności nie muszą należeć do najniższych.

Szybkość działania algorytmu jest krytycznym parametrem z uwagi na częste zastosowanie danych multimedialnych w aplikacjach czasu rzeczywistego oraz ich dużą objętość. Wyróżnia się czas potrzebny na przeprowadzenie procesu szyfrowania oraz czas niezbędny do określenia danych, które mają podlegać szyfrowaniu [UhPo05].

Czynnikami różnicującymi poszczególne algorytmy są:

- przezroczystość – zaszyfrowany materiał multimedialny jest dekodowalny w odbiorniku nawet bez znajomości klucza szyfrującego; w odbiorniku znana jest informacja o strukturze składni pliku lub strumienia, ponieważ ten element nie jest szyfrowany;
- skalowalność – wielopoziomowe zabezpieczenia dla różnych aplikacji z elastycznie dobieranymi wartościami parametrów; jest ona realizowana przez szyfrowanie wybranych warstw lub ich fragmentów, na przykład w standardzie JPEG2000 czy MPEG 2/4; pozwala kontrolować jakość zaszyfrowanych danych multimedialnych;

*) Bezpośrednie szyfrowanie i skramblowanie zostały przedstawione jako odniesienie w stosunku do innych klas algorytmów

– dostrzegalność – uogólnienie wielowarstwowego (skalowalnego) szyfrowania, niezależne od wielowarstwowej struktury wbudowanej w zaszyfrowany obraz, oparte na częściowym szyfrowaniu obrazu czy wideo;
– tolerancja błędów – wprowadzenie do algorytmów szyfrowania udogodnień mających na celu podniesienie odporności na błędy, a tym samym zapewnienie prawidłowego przebiegu deszyfrowania [FuKi05].

3. Główne klasy algorytmów

3.1. Bezpośrednie szyfrowanie

Bezpośrednie szyfrowanie strumienia ciągu danych wejściowych tradycyjnymi metodami jest bardziej odpowiednie dla danych tekstowych i danych multimedialnych o niskiej jakości. Tego typu metody nazywane są w literaturze podejściem naiwnym (ang. *naive approach*) [FuSo04] i wykorzystują algorytmy symetrycznego szyfrowania. Ich przykładem jest szyfrowanie pakietów w czasie rzeczywistym za pomocą protokołu SRTP (ang. *Secure Real-time Transport Protocol*), który opiera się na szyfrze AES (ang. *Advanced Encryption Standard*), znanym również jako Rijndael.

3.2. Skramblowanie

Zastosowanie do całego strumienia ma również skramblowanie (ang. *scrambling*) [FuSo04]. Skramblowanie opiera się na prostych szyfrach podstawieniowych i przestawieniowych, oferujących bardzo niskie bezpieczeństwo. Innym sposobem skramblowania jest dokonywanie przekształceń na analogowym sygnale w dziedzinie czasu albo częstotliwości. Skramblowanie obniża stopień kompresji, ponieważ zaburza statystykę oryginalnych danych, na których bazuje algorytm kompresji.

3.3. Selektywne szyfrowanie

Właściwości wymienione w punkcie 1 wymuszają potrzebę zastosowania algorytmów kryptograficznych zapewniających mniejszy koszt obliczeniowy poprzez selektywne operowanie tylko niektórymi częściami strumienia bitów, bezpośrednio związanymi z przenoszoną informacją. Technika ta nosi nazwę selektywnego, częściowego, szyfrowania (ang. *selective encryption*).

Określone algorytmy selektywnego szyfrowania są najczęściej zoptymalizowane dla wąskiej grupy zastosowań [Look03]. Istnieje możliwość używania różnych algorytmów selektywnego szyfrowania dla pojedynczego strumienia bitów. Z drugiej strony, dany proces częściowego szyfrowania może współpracować ze stałym algorytmem kompresji lub algorytm ten, w szczególności jego parametry, podlegają modyfikacji.

Algorytmy selektywnego szyfrowania można dzielić, biorąc pod uwagę:
– typ danych wejściowych: obraz, wideo, audio, mowa;
– sposób reprezentacji informacji – dziedzina: przestrzenna; transformaty: DCT, falkowa, DFT, kodera entropijnego;
– postać danych wejściowych: szyfrowanie operujące danymi skompresowanymi (ang. *compressed oriented schemes*), szyfrowanie operujące strumieniem bitowym lub danymi w postaci jawnej (ang. *bitstream oriented schemes*) [FuKi05, UhPo05].

Schematy zorientowane bitowo mogą być zastosowane w usłudze wideokonferencji, natomiast zorientowane kompresyjnie – w aplikacjach VoD.

W porównaniu z podejściem naiwnym, użycie selektywnego szyfrowania jest zasadne, gdy suma czasu potrzebnego do zidentyfikowania wymaganych właściwości danych oraz przebiegu samego algorytmu jest znacznie mniejsza od czasu bezpośredniego zaszyfrowania.

Istniejące algorytmy selektywnego szyfrowania pracują najczęściej w dziedzinie transformaty DCT, falkowej oraz w odniesieniu do danych wideo.

Ponadto występuje szereg algorytmów, które mogą być zastosowane zarówno do szyfrowania obrazu, jak i danych wideo [FuKi05]. Dotyczy to m.in. algorytmów:
– opartych na transformacie DCT, wykorzystywanej w standardach JPEG, MPEG;
– szyfrowania obrazów, związanych z transformatą falkową, które są rozwijane w kierunku szyfrowania wideo (Motion-JPEG2000);
– zapewniających poufność procesu kodowania entropijnego podczas kompresji obrazu i wideo.

3.4. Schematy szyfrowania bazujące na chaosie

Kryptosystemy chaotyczne (ang. *chaos cryptosystems*), wykorzystujące teorię chaosu, są również stosowane do szyfrowania obrazu czy wideo. Wyróżnia się dwie gałęzie zastosowań chaosu do szyfrowania obrazów i wideo [FuKi05]. Chaos może być użyty do generacji bitów pseudolosowych, o założonych właściwościach statystycznych, lub do realizacji permutacji poprzez włączenie dwuwymiarowych map chaosu lub krzywych fraktalnych. Pierwsza metoda jest stosowana do projektowania chaotycznych szyfrów strumieniowych, a druga do schematów szyfrowania obrazów bazujących na chaosie. Kompresja jest stosowana głównie w algorytmach z krzywymi fraktalnymi, tzw. SCAN.

3.5. Kompresja w znakowaniu wodnym

Najważniejszą klasą algorytmów służących do otrzymywania odwracalnych znaków wodnych (ang. *reversible watermarks*) są algorytmy oparte na kompresji, należące do technik kodowania transformującego i przestrzennego [FuKi05]. Odwracalne znakowanie wodne daje możliwość usunięcia znaku wodnego wraz ze zniekształceniami wynikającymi z jego uprzedniego wstawienia, czyli możliwość całkowitego odwrócenia procesu znakowania oraz umieszczania dużej ilości danych w obrazie, rzędu setek kB.

W odwracalnym znakowaniu wodnym, bazującym na kompresji, dochodzi do zamiany nieznaczących cech obrazu na sekwencję pseudolosową w procesie wstawiania znaku. Cecha pseudolosowa jest utworzona przez strumień bitów złożony z tzw. *payloadu* (znaku wodnego) i skompresowanej – dla zapewnienia odwracalności – nieznaczącej, oryginalnej cechy obrazu. W celu odtworzenia oryginalnego obrazu najpierw pozyskiwana jest sekwencja pseudolosowa, a następnie oryginalna cecha obrazu jest otrzymywana ze złożonego strumienia bitów dzięki zastosowaniu dekompresji. Ostatecznie sekwencja pseudolosowa jest zamieniana na oryginalną cechę obrazu.

Często stosowane jest wbudowywanie znaku wodnego we współczynniki transformat materiału audio w celu zwiększenia

zasięgu znaku oraz podniesienia odporności na ataki geometryczne (np. zmodyfikowane DCT, MDCT) [FuKi05]. Transformaty są często wykorzystywane przy wstawianiu znaku wodnego z uwagi na to, że przetwarzanie przez nie sygnałów, obejmujące kodowanie i kompresję, jest popularne. Proces wbudowywania znaku wodnego może być łatwo zintegrowany z istniejącymi schematami kodowania, bez wykonywania dodatkowych przekształceń czy obliczeń.

W dziedzinie znakowania wodnego często podnoszona jest kwestia odporności wstawionego znaku wodnego na zniekształcenia, wynikające m.in. z działania algorytmów kompresji.

3.6. Ukrywanie danych

Opisywane w poprzednim punkcie znakowanie wodne jest szczególnym przypadkiem technik ukrywania danych (ang. *data hiding*).

Z kompresją związane są algorytmy bezstratnego ukrywania danych [FuKi05], tzn. odwracalnego, prowadzącego do otrzymania oryginalnej postaci medium pokrywającego. Są nimi: kruche uwierzytelnianie (ang. *fragile authentication*), algorytmy o wysokiej pojemności wbudowywania (ang. *high embedding capacity*), półkruche uwierzytelnianie (ang. *semi-fragile authentication*).

W klasie algorytmów kruchego uwierzytelniania (gdzie dane uwierzytelniające szybko tracą swoją przydatność już w wyniku drobnych modyfikacji medium kryjącego) stosuje się bezstratną kompresję bitów oryginalnego obrazu w celu utworzenia miejsca na wstawienie ukrytych danych. Przykładowo, znane jest rozwiązanie bazujące na bezstratnej kompresji przesuniętych strumieni bitowych, otrzymanych ze skwantowanych współczynników JPEG.

Z kolei algorytmy prowadzące do wysokiej objętości wbudowanych danych mogą wykorzystywać bezstratną kompresję współczynników transformat falkowych lub skwantowanych wartości obrazu.

W półkruchym uwierzytelnianiu rozpatrywana jest głównie kwestia odporności tego typu algorytmów na niewielkie modyfikacje materiału multimedialnego, związane z obydwoma rodzajami kompresji, nie wprowadzające zasadniczych różnic w stosunku do oryginalnej postaci zawartości multimedialnej.

3.7. Test pseudolosowości Lempela-Ziva

Kompresja jest zastosowana w teście pseudolosowości Lempela-Ziva, należącym do grupy 16 testów opublikowanych przez organizację NIST i służących do badania pseudolosowości sekwencji binarnych o określonej długości utworzonych przez generatory liczb pseudolosowych. W teście Lempela-Ziva bada się, w jakim stopniu sekwencja wejściowa daje się kompresować, przy czym sekwencja pseudolosowa powinna podlegać kompresji co najwyżej w niewielkim stopniu. Opis testu wraz z proponowanymi w stosunku do niego poprawkami można znaleźć w pracy pt. *Corrections of the NIST Statistical Test Suite for Randomness* [KiUm04].

3.8. Inne algorytmy kryptograficzne wykorzystujące kompresję

W tym podpunkcie [Avan05] zostaną przedstawione algorytmy kryptograficzne wykorzystujące kompresję, lecz rozumianą odmiennie w stosunku do klasycznych jej rozwiązań, stosowanych w dziedzinie multimediów – kompresję używaną w kryptografii torusowej (ang. *torus-based cryptography*) oraz kryptografii krzywych eliptycznych (ang. *elliptic curve cryptography*) [Avan05].

Kryptografia torusowa służy do projektowania kryptosystemów opartych na grupach o specjalnych właściwościach i problemie logarytmu dyskretnego. Kompresja w kryptografii torusowej prowadzi do otrzymania zwartej reprezentacji danej półgrupy, której elementy należą do torusa. Przykładem tego typu kryptosystemów są XTR oraz CEILIDH, które znajdują zastosowanie przy ulepszaniu znanych algorytmów z kluczem publicznym.

W dziedzinie krzywych eliptycznych, gdzie problem logarytmu dyskretnego rozwiązuje się w odniesieniu do takiej krzywej, a nie do skończonego ciała, skompresowaną postać otrzymuje się poprzez zadanie współrzędnej x oraz bitu określającego, które z maksymalnie dwóch rozwiązań jest właściwe dla równania kwadratowego opisującego daną krzywą. Dla krzywych eliptycznych wyższego rzędu podaje się z kolei wielomian $p(x)$ stopnia co najwyżej n oraz n bitów dla określenia odpowiednich rozwiązań.

4. Przykłady algorytmów selektywnego szyfrowania

4.1. Szyfrowanie transparentne obrazów

Transparentne szyfrowanie (ang. *transparent encryption*) wiąże się z szyfrowaniem warstw wzbogacających (ang. *enhancement layers*) skalowalnego strumienia bitowego, które zawierają dane służące do podniesienia jakości obrazu lub wideo w stosunku do niskiej jakości reprezentowanej przez warstwę bazową (ang. *base layer*) [UhPo05]. Transparentne szyfrowanie znajduje zastosowanie w aplikacjach, w których materiał o niskiej jakości jest dostępny dla każdego, natomiast pełna jakość obrazu lub wideo jest osiągalna przez użytkowników po wniesieniu opłaty. Przykładami mogą być cyfrowa telewizja rozsiewcza lub efektywne przeglądanie multimedialnych baz danych.

W pracy pt. *Techniques for selective encryption of uncompressed and compressed images* [DrBe02] zaproponowano szyfrowanie bitplanów oryginalnego obrazu począwszy od najmniej znaczących bitów. Zaszyfrowanie co najmniej 4–5 najmniej znaczących bitplanów spośród 8 bitplanów obrazu w skali szarości, będących danymi słabo skorelowanymi z oryginalnym obrazem o charakterze zbliżonym do losowego, powoduje widoczną degradację obrazu oraz wykazuje odporność na ataki z otwartym tekstem jawnym. Funkcją szyfrującą jest XOR (czyli alternatywa wykluczająca), a długość klucza jest równa rozmiarowi szyfrowanych danych obrazu. Jednakże częściowa utrata jakości obrazu nie jest wystarczająca dla aplikacji wymagających wysokiego poziomu bezpieczeństwa.

W obrazach skompresowanych JPEG szyfrowaniu podlegają dodatkowe bity znaku oraz wartości bezwzględnej określonej liczby niezerowych współczynników AC [DrBe02]. Nie są szyfrowane słowa kodowe, ponieważ uczestniczą one w procesie synchronizacji, a także nie ma sensu zamienianie zerowych współczynników z niezerowymi współczynnikami oraz współczynników DC, których wartości są wysoce przewidywalne. Liczba niezaszyfrowanych współczynników powinna być mniejsza niż pięć (włącznie ze współczynnikiem DC). Algorytm może być przeprowadzany na określonych zbiorach współczynników danego obrazu przy wykorzystaniu

różnych kluczy [Droo04]. Jeżeli zbiory te są odmienne, to stosuje się wielokrotne selektywne szyfrowanie, natomiast gdy zbiory te pokrywają się, to należy użyć schematu $E_{k1}(D_{k2}(E_{k1}(f)))$ zwanego nad-szyfrowaniem (ang. *over-encryption*). Po procesie szyfrowania standardowym szyfrem blokowym (np. 3DES) następuje zamiana bitów w strumieniu bitowym w celu zapewnienia zgodności jego ostatecznej postaci z formatem wymaganym przez dany system kompresji.

Pierwszy z opisanych algorytmów szyfrowania obrazów operuje w dziedzinie przestrzennej na strumieniu bitowym, a drugi, w dziedzinie transformaty DCT, na danych skompresowanych algorytmem JPEG.

4.2. Szyfrowanie obrazów i danych wideo

W pracy pt. *Partial Encryption of Compressed Images and Videos* [ChLi00] przedstawiono sposób szyfrowania obrazów skompresowanych falkowo oraz jego rozszerzenie, służące do zabezpieczania materiału wideo. W obydwóch przypadkach dane są skompresowane algorytmem SPIHT, bazującym na drzewie zerowym.

Metoda przedstawiona w tej pracy polega na szyfrowaniu istotnych bitów, reprezentujących istotne zbiory lub piksele, które należą do dwóch najwyższych poziomów piramidy, jak również parametr n, określający początkowy próg istotności. Nie ma potrzeby szyfrowania wszystkich pozostałych danych, ponieważ są one otrzymywane w wyniku dekompozycji zbiorów leżących w dwóch pierwszych podpasmach (inicjalizacji różnych list wykorzystywanych przez algorytm). Wspomniane zaszyfrowane istotne bity nie mogą być odgadnięte poprzez obserwację bitów należących do niższych poziomów piramidy.

Ilość zaszyfrowanych danych jest więc niewielka, rzędu kilku procent. Algorytmem szyfrującym może być AES.

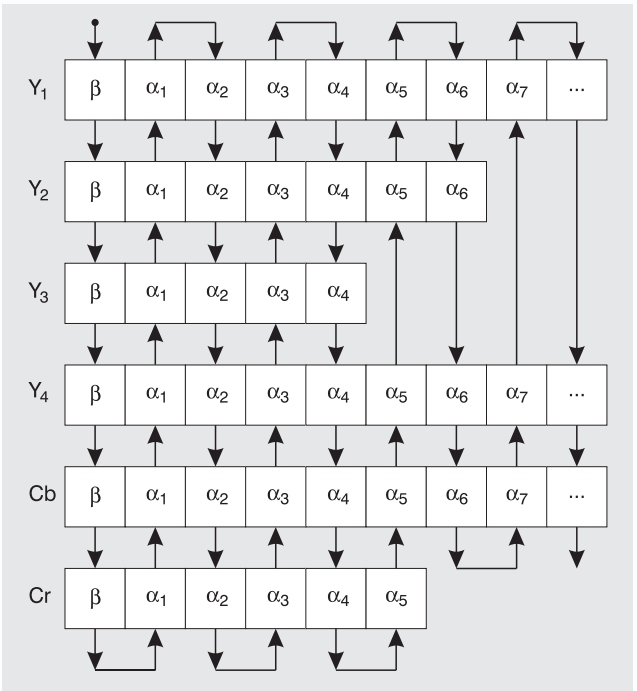
Powyższa metoda szyfrowania obrazu może być zastosowana również w odniesieniu do danych wideo posiadających niskie rozdzielczości, występujących np. w usłudze wideotelefonii. Cel zostaje osiągnięty przez szyfrowanie ramek typu I, wektorów ruchu oraz błędów predykcji. Zabezpieczanie dwóch pierwszych elementów pozwala uniknąć uzyskania aproksymacji kolejnych ramek przez atakującego, natomiast szyfrowanie błędu predykcji – uzyskania informacji o zarysach poruszających się obiektów, nie będących dokładnie przewidywanymi przez wektory ruchu.

4.3. Szyfrowanie sekwencji wideo

Schematy selektywnego szyfrowania danych wideo skompresowanych algorytmem MPEG opierają się najczęściej na zabezpieczaniu określonych makrobloków, ramek, współczynników DCT oraz wektorów ruchu i mogą nie zapewniać odpowiedniego poziomu bezpieczeństwa wskutek rozproszenia informacji widzialnej na wszystkie współczynniki DCT i ich poszczególne bity bądź ograniczenia szyfrowania tylko do ramek typu I [FuKi05]. Ponadto szyfrowanie nagłówków w tychże schematach powoduje utratę zgodności z formatem MPEG.

Z kolei metody polegające na poufnych permutacjach wszystkich lub wybranych makrobloków, bloków, współczynników DCT i wektorów ruchu bywają podatne na ataki: z szyfrogramem, a także ze znanym i wybranym tekstem jawnym [FuKi05].

Jednym z algorytmów operujących na danych wideo w standardzie MPEG, pozbawionym powyższych wad, jest RVEA (ang. *Realtime Video Encryption Algorithm*) [BhSh02]. Metoda ta szyfruje wybrane bity znaku współczynników DCT oraz wektorów ruchu dowolnym, znanym szyfrem blokowym. W końcowym etapie algorytmu zaszyfrowane bity znaku są umieszczane z powrotem na pozycjach, z których zostały pobrane.



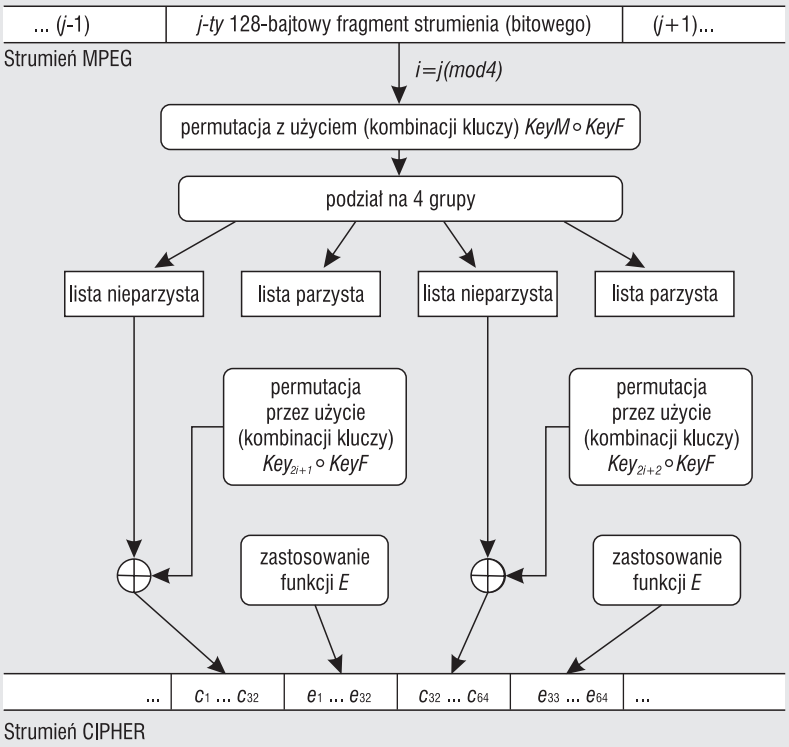
Rys. 1. Sposób wyboru bitów znaku współczynników DCT w algorytmie RVEA [FuKi05]

W trakcie przebiegu algorytmu, dla każdego makrobloku wybieranych jest do:

- 64 bitów znaku współczynników DCT w przypadku ramek I,
- 62 bitów znaku współczynników DCT oraz bity znaku wektora ruchu w przód w przypadku ramek P,
- 60 bitów znaku współczynników DCT oraz bity znaku wektora ruchu w przód i w tył w przypadku ramek B.

Sposób wyboru bitów znaku współczynników DCT jest przedstawiony na rys. 1, gdzie: Y_i – bloki luminancji 8 x 8 pikseli, C_b i C_r – bloki chrominancji 8 x 8 pikseli, β – kody współczynników DC, α_i – kody i-tych niezerowych współczynników AC. Metoda wyboru jest uzależniona od spostrzeżenia, że współczynniki DC oraz AC wyższych częstotliwości są bardziej znaczące od współczynników AC niższych częstotliwości (wektory ruchu są bardziej znaczące od współczynników DCT).

Ograniczenie czasu trwania obliczeń jest uzyskiwane przez wybór skończonej liczby bitów. Bity znaku zajmują 10% całkowitego strumienia bitowego, dlatego za pomocą RVEA można zaoszczędzić 90% czasu obliczeń w porównaniu z szyfrowaniem bezpośrednim. Czas przetwarzania algorytmem RVEA jest zawsze krótszy, niezależnie od rozmiaru i rodzaju ramki.



Rys. 2. Algorytm VEA [QiNa97]

Szyfrowany może być również strumień wideo (rys. 2) [QiNa97]. Poszczególne etapy są następujące:

1) utworzenie bloku nagłówka dla każdej ramki MPEG typu I;
2) dodanie *KeyF* do *KeyM* i Key_i;
3) obliczenie dla $i=j$ (mod4) dla j-tego 128-bitowego segmentu strumienia bitowego;
4) mieszanie j-tego 128-bajtowego segmentu strumienia bitowego z kluczem *KeyM* *KeyF* i podział wynikowego segmentu na cztery kolejne 32-bajtowe części, gdzie pierwsza i trzecia część tworzy dwie Listy Nieparzyste, a druga i czwarta – dwie Listy Parzyste;
5) mieszanie pierwszej Parzystej Listy z kluczem Key_{2i+1} *KeyF*; wynikowa Parzysta Lista jest:
   a) ksorowana (poddawana działaniu funkcji XOR) z pierwszą Nieparzystą Listą, dając szyfrogram w postaci *c1 c2 … c32*;
   b) szyfrowana funkcją *E* przy wykorzystaniu klucza *KeyE*, dając szyfrogram *E1 E2 … E32*; zastosowanie tych samych kroków do innych par List Parzystych i Nieparzystych;
6) powtórzenie kroku 3.;
7) powtórzenie kroku 1. dla każdej ramki.

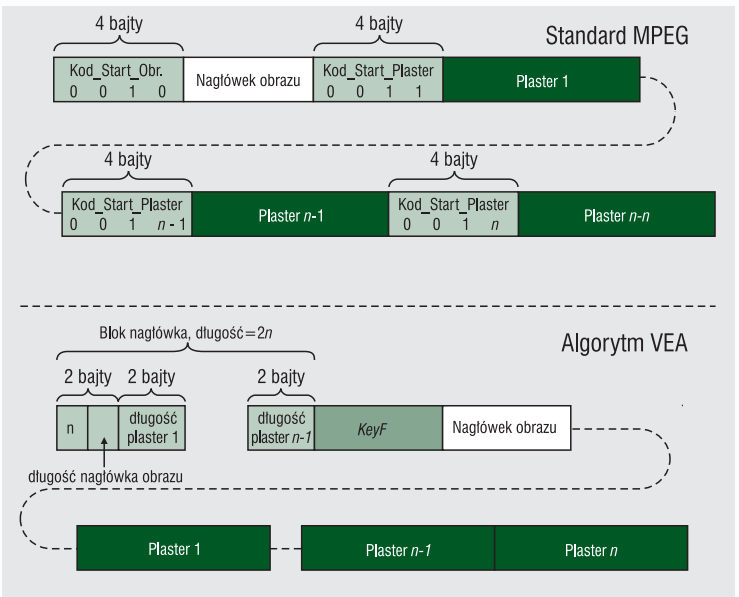
KeyF jest kluczem 64-bitowym, przydzielanym każdej ramce, dołączanym do kluczy *KeyM* i Key_i w celu otrzymania nowych kluczy dla tejże ramki: *KeyM* *KeyF* Key_i *KeyF* oraz wprowadzenia dalszego zróżnicowania wyboru Listy Nieparzystej i Parzystej.

KeyM składa się ze 128 bitów – 64 zer i 64 jedynek. Jeżeli i-ty bit klucza *KeyM* jest równy 1, to i-ty bajt 128-bajtowego segmentu jest zaliczany do Listy Nieparzystej.

Key_i to osiem kluczy. Każdy z nich ma długość 20 bajtów i służy do mieszania jednej z ośmiu części w celu uzyskania niepowtarzalności wartości bajtów w obrębie połowy ramki. Key_1 jest stosowany do pierwszych 32 bajtów Listy Nieparzystej, Key_2 do kolejnych 32 bajtów itd.

W algorytmie VEA używana jest zmodyfikowana postać nagłówka ramki MPEG (rys. 3), ponieważ strumień wideo jest indeksowany oraz transmitowany ramka po ramce i nie są potrzebne 4-bajtowe pola startu obrazu oraz segmentu [QiNa97]. Pola te mogą natomiast zostać wykorzystane do przechowania informacji o kluczu *KeyF*, liczbie segmentów w ramce, odległości między kodem startu obrazu a pierwszym segmentem, długości każdego segmentu. W trakcie dekodowania ramki dochodzi do umieszczenia sekwencji 0010 jako kodu startu obrazu, rekonstrukcji kodów startu segmentów, umieszczenia ich na oryginalnych pozycjach na podstawie długości segmentu i otrzymania klucza *KeyF*. Blok nagłówka oraz klucz *KeyF* są zaszyfrowane z użyciem klucza *KeyE*. Nagłówki obrazów MPEG nie są szyfrowane, ponieważ zawierają informacje, które są bezwartościowe w przypadku braku znajomości danych użytkowych, czyli współczynników DCT (np. dotyczące rozmiaru obrazu i szybkości transmisji obrazu).

Szybkość działania algorytmu jest dwa razy szybsza w porównaniu z podejściem naiwnym, a jego bezpieczeństwo zależy od funkcji E, którą jest szyfr blokowy.



Rys. 3. Postać bloku nagłówka ramki MPEG używana w algorytmie VEA [QiNa97]

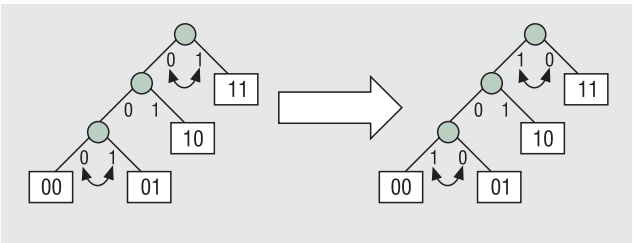
4.4. Zabezpieczanie kodera entropijnego

Kodowanie entropijne jest stosowane w standardach JPEG i MPEG. Algorytm zapewniający poufność kodowania entropijnego może wykorzystywać wielokrotne tablice Huffmana [XiKu04], gdzie na podstawie losowego indeksu, pełniącego rolę tajnego klucza, dochodzi do wyboru określonego drzewa Huffmana dla danego słowa kodowego.

Procedura kodowania entropijnego, opartego na wielokrotnych tablicach Huffmana, jest następująca:

1) generacja 2^k różnych tablic Huffmana, ponumerowanych od 0 do 2^k–1,
2) generacja m-bitowej sekwencji pseudolosowej s,
3) obliczenie $r=[m/k]$
4) obliczenie $h(s)=t_1\|t_2\| \ \ldots \ \|t_r\|rem$, gdzie: t_i jest liczbą od 0 do n–1, wyrażoną za pomocą k-bitów, rem – pozostałe bity, jeśli m nie jest wielokrotnością k,
5) dla każdego i, gdzie $i=1,2, \ldots r$, użycie tablicy t_i do zakodowania pojedynczego symbolu,
6) ustawienie $s=s+1$, po zakodowaniu r symboli, i powrót do kroku 4.

Tablice Huffmana mogą być generowane przy użyciu zbiorów obrazów treningowych lub procesu mutacji drzewa Huffmana [WuKu01]. Poszczególne tablice Huffmana muszą pochodzić z różnych zbiorów treningowych, aby nie doszło do zmniejszenia stopnia kompresji.

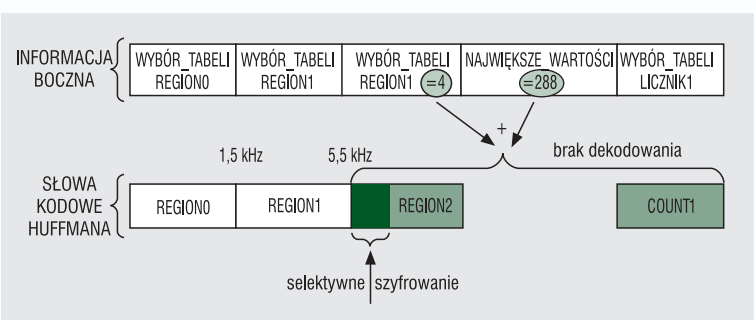


Rys. 4. Proces mutacji drzewa Huffmana [WuKu01]

Proces mutacji drzewa Huffmana (rys. 4) polega na tworzeniu kolejnych tablic Huffmana w wyniku zmiany etykiet gałęzi czterech bazowych optymalnych drzew Huffmana. Jeżeli dane drzewo bazowe posiada m liści, to możliwe jest otrzymanie 2^{m-1} różnych tablic Huffmana. Modyfikowane są te pary etykiet, którym odpowiadają zerowe bity w losowo wygenerowanej $(m–1)$-bitowej liczbie całkowitej.

4.5. Szyfrowanie danych audio

Zabezpieczenie danych audio, skompresowanych algorytmem MPEG Layer III, może opierać się na modyfikacji i zaszyfrowaniu określonych pól ramki MP3 [SeTe03]. Optymalne pod względem liczby szyfrowanych bitów oraz wielkości wprowadzanych zniekształceń sygnału audio jest szyfrowanie zaledwie jednego bitu z pola REGION1 oraz umożliwienie dekodowania bitów zawartych tylko w polu REGION0, ponieważ nawet niewielka modyfikacja w region1 wprowadza zauważalne zniekształcenia sygnału.



Rys. 5. Szyfrowanie ramki MP3 [SeTe03]

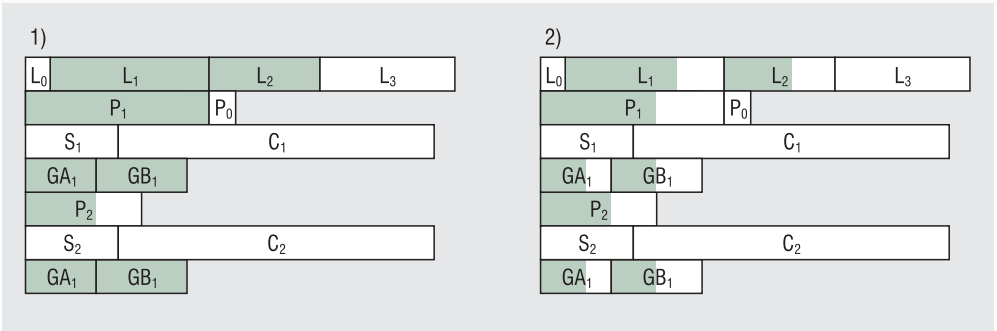
Znacznie bardziej bezpieczne jest szyfrowanie 70–100 bitów zawartych w REGION2 i jednoczesne dekodowanie bitów zawartych w polach REGION0 i REGION1 (rys. 5). Szyfrogram zajmuje wtedy 6,3–8,3% objętości strumienia bitowego, próbkowanego z częstotliwością 44,1 kHz, o przepływności 128 kbit/s. Pola REGION0–REGION2 zawierają zakodowane trzema różnymi kodami Huffmana największe wartości współczynników zmodyfikowanego przekształcenia kosinusowego, które odpowiadają najniższym częstotliwościom. Dekompresja, ograniczona do współczynników leżących w REGION0 i REGION1, jest równoważna filtracji dolnoprzepustowej sygnału audio. Prowadzi ona do otrzymania sygnału o obniżonej jakości. Ponadto rekonstrukcja zaszyfrowanych wartości współczynników MDCT wywołuje błędy synchronizacji, dlatego też obszar ramki MP3, który ma być zaszyfrowany, powinien być ominięty przez dekoder. W przypadku pola REGION2 efekt ten zostaje osiągnięty przez ustawienie wartości 4 w WYBÓR_TABELI REGION2. Z kolei poprzez wpisanie wartości 288 w pole NAJWIĘKSZE_WARTOŚCI dochodzi do jego maksymalnego wydłużenia aż do końca pasma o wartość pola LICZNIK1, które zwyczajowo przechowuje wartości współczynników z przedziału <-1; 1>. W celu odzyskania oryginalnej postaci ramki MP3 należy na początku ścieżki audio dołączyć dodatkowy zaszyfrowany nagłówek, zawierający dane o wcześniejszych wartościach WYBÓR_TABELI oraz NAJWIĘKSZE_WARTOŚCI.

Opisany algorytm działa również w dziedzinie transformaty DCT.

4.6. Szyfrowanie mowy w standardzie G.729

W pracy pt. *Frequency-Selective Partial Encryption of Compressed Audio* [SeTe02] zaproponowano dwa algorytmy szyfrowania mowy w standardzie G.729, operującym z szybkością 8 kb/s. Pierwsza z metod ma na celu degradację mowy pozwalającą uniknąć bezpośredniego podsłuchu, który może stać się możliwy dopiero po odpowiedniej kryptoanalizie. Drugi z algorytmów szyfruje więcej, to jest około połowy strumienia bitowego, i zapewnia wyższy poziom bezpieczeństwa, porównywalny z tym, jaki jest oferowany w podejściu naiwnym. Wybór liczby szyfrowanych bitów został przeprowadzony doświadczalnie, z uwzględnieniem znaczenia percepcji poszczególnych parametrów wyjściowych kodeka G.729, takich jak: wpływ obwiedni widmowej na zrozumiałość, rola wzmocnienia przy rozróżnianiu mowy dźwięcznej i bezdźwięcznej oraz mowy i ciszy, okres wysokości dźwięku, identyfikacja płci. Większy ze zbiorów bitów obejmuje: indeksy kwantyzacji wektorowej L1 i L2, liniowe częstotliwości widmowe, pierwszych siedem najbardziej znaczących bitów wartości kwantyzowanego okresu wysokości dźwięku, pierwsze trzy najbardziej

znaczące bity różnicowo kwantyzowanego okresu wysokości dźwięku, cztery indeksy wektora wzmocnienia. W drugim zbiorze dla wymienionych parametrów szyfrowanych jest mniej bitów, z wyjątkiem różnicowo zakodowanego okresu wysokości dźwięku.



Rys. 6. Zaszyfrowanie bity poszczególnych parametrów wyjściowych kodeka G.729 [SeTe02]

5. Podsumowanie

W artykule została omówiona problematyka adaptacji poziomu zabezpieczeń danego rodzaju materiału multimedialnego do warunków sieciowych oraz możliwości urządzeń końcowych. Jest ona związana głównie z zagadnieniami bezpiecznego skalowalnego streamingu i transkodingu, służącego do zapewniania poufności oraz uwierzytelniania.

Rozwiązania przedstawione w pierwszej części artykułu charakteryzują się znacznym zmniejszeniem ilości przetwarzanych danych i skróceniem czasu obliczeń w porównaniu z szyfrowaniem całości materiału multimedialnego. Znajdują one zastosowanie w zabezpieczaniu danych wideo, obrazu, audio i mowy, a tym samym usług multimedialnych, takich jak wideokonferencje, wideo na życzenie, telewizja rozsiewcza, multimedialne bazy danych. Algorytmy selektywnego szyfrowania wpływają na stopień kompresji w niewielkim zakresie, co jest również pożądane, zwłaszcza przy zapewnianiu bezpieczeństwa usług wymagających większych przepływności. Selektywne szyfrowanie danych wideo może wykazywać podatności być podatne na ataki, nie zapewniać odpowiedniego poziomu ochrony danych, a także skutkować utratą zgodności z formatem MPEG.

PIOTR PIOTROWSKI
INSTYTUT TELEKOMUNIKACJI, WYDZIA ELEKTRONIKI I TECHNIK INFORMACYJNYCH, POLITECHNIKA WARSZAWSKA
P.T.PIOTROWSKI@ELKA.PW.EDU.PL

Literatura:

[Avan05] Avanzi R.: *D. AZTEC. 2. Alternatives to RSA (Lightweight Asymmetric Cryptography and Alternatives to RSA)*, ECRYPT, August 2005.

[BhSh02] Bhargava B., Shi C., Wang S.: *MPEG Video Encryption Algorithms,* 2002.

[ChLi00] Cheng H., Li X.: *Partial Encryption of Compressed Images and Videos*, IEEE Trans. Signal Process., 48(8), 2439-2451, 2000.

[DrBe02] Van Droogenbroeck M., Benedett R.: *Techniques for selective encryption of uncompressed and compressed images*, Proceedings of ACIVS 2002 (Advanced Concepts for Intelligent Vision Systems), Ghent, Belgium, September 2002.

[Droo04] Van Droogenbroeck M.: *Partial encryption of images for real-time applications*, Liege, Belgium 2004.

[FuKi05] Furht B., Kirovski D.: *Multimedia Security Handbook*, CRC Press, 2005.

[FuSo04] Furht B., Socek D.: *A Survey of Multimedia Security*, Comprehensive Report on Information Security, IEC 2004.

[KiUm04] Kim S., Umeno K., Hasegawa A.: *Corrections of the NIST Statistical Test Suite for Randomness*, Cryptology ePrint Archive, January 2004.

[Look03] Lookabaugh T. D. i inni: *Security Analysis of Selectively Encrypted MPEG-2 Streams*, Proceedings of the SPIE, Vol. 5241, pp. 10-21, November 2003.

[ÖzSo04] Öztürk I., Sogukpinar I.: *Analysis and Comparison of Image Encryption Algorithms*, International Journal of Information Technology, Vol. 1, No. 2, 2004.

[QiNa97] Qiao L., Nahrstedt K.: *A New Algorithm for MPEG Video Encryption*, Proceedings of the 1st International Conference on Imaging Science, Systems and Technology, 1997, pp. 21-29.

[SeTe02] Servetti A., De Martin J. C.: *Perception-Based Partial Encryption of Compressed Speech*, IEEE Transactions of speech and audio processing, Vol. 10, No. 8, 2002.

[SeTe03] Servetti A., Testa C., De Martin J. C., „Frequency-Selective Partial Encryption of Compressed Audio", IEEE International Conference on Acoustics, Speech and Signal Processing, Hong-Kong, 2003.

[UhPo05] Uhl A., Pommer A.: *Image and Video Encryption. From Digital Rights Management to Secured Personal Communication*, Springer, 2005.

[Wang05] Wang C.: *Cryptography in Data Compression*, CodeBreakers-Journal, Vol. 2, No. 3, 2005.

[WuKu00] Wu C.-P., Kuo C.-C. J.: *Fast Encryption Methods for Audiovisual Data Confidentiality*, Proceedings of the SPIE, Vol. 4209, pp. 284-295, November 2000.

[WuKu01] Wu C.-P., Kuo C.-C. J. *Efficient Multimedia Encryption via Entropy Codec Design*, Proceedings of the SPIE Security and Watermarking of Multimedia Content III, San Jose 2001, Vol. 4314.

[XiKu04] Xie D., Kuo C.-C. J.: *Enhanced multiple Huffman table (MHT) encryption scheme using key hopping*, ISCAS (5) 2004, pp. 568-571.

Obiektywnie patrząc najlepszy

Computar – szeroka gama
najczęściej na świecie kupowanych obiektywów CCTV.

computar®

CBC GROUP

CBC (Poland) Sp. z o.o., ul. Gustawa Morcinka 5/6, 01-496 Warszawa,
tel.: (0 22) 638 44 40, faks: (0 22) 638 45 41, www.cbcpoland.pl, e-mail: info@cbcpoland.pl

DOSKONAŁA FUNKCJONALNOŚĆ ZA NIESPOTYKANĄ CENĘ

24M.pl

wyłączny przedstawiciel producenta w Polsce

2399 PLN netto

obsługa przez mysz

Rejestratory MPEG4, triplex, VGA 4 x audio, LAN, polskie menu

REJX16

REJX4

1299 PLN netto

- polskie menu
- obsługa myszką, z panela lub pilotem
- 4 niezależne kanały audio
- pokrętło jog shuttle do przewijania nagrań
- ustawiane dla każdej kamery i godziny:
  - rozdzielczość
  - jakość nagrania
  - ilość klatek
- grupy użytkowników z różnymi uprawnieniami
- zdalna konfiguracja przez sieć
- triplex
- programowane wyjście SPOT
- wyjście VGA i s-video
- dwukierunkowa komunikacja głosowa
- pilot
- wersje z DVD lub CD

zobacz online:
www.24m.pl/rejx4

Specyfikacja

Cecha	REJX16	REJX4
wejścia video	16 x BNC przelotowe	4 x BNC
wejścia audio	4 x chinch	4 x chinch
wyjścia video	1 x BNC, 1x spot-out, 1 x VGA, 1x s-video	1 x BNC, 1x spot-out, 1 x vga, 1x s-video
wyjścia audio	1 x chinch	1 x chinch
kompresja video	MPEG4	MPEG4
rozdzielczość	704 x 576, 704 x 288, 352 x 288	704 x 576, 704 x 288, 352 x 288
szybkość odtwarzania	400 klatek / s [16 x 25]	100 klatek / s [4 x 25]
tryb nagrywania	ciągły, detekcja, alarm, harmonogram, kryzysowy	ciągły, detekcja, alarm, harmonogram
konfiguracja przez sieć	tak	tak
nośnik	3 x HDD 3,5" ATA [bez limitu]	2 x HDD 3,5" ATA

automatyczne zaznaczanie obszarów w których wykryto ruch

intuicyjne menu graficzne

menu w języku polskim

precyzyjny harmonogram pracy

filtr powiadomień mailowych

dostępne wersje z CD i DVD

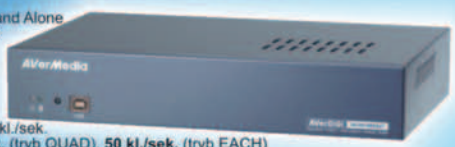
24M.pl tel. 071 333 87 22, 071 724 52 82, 0601 24 66 66, poczta@24m.pl, **www.24m.pl**

INFO-CAM

Wyłączny dystrybutor **AVerMedia Technologies, Inc.** www.infocam.com.pl

PŁOCK Al. Kilińskiego 5, tel. (024) 266 97 12, tel./fax (024) 266 97 13, handlowy@infocam.com.pl
POZNAŃ ul. Opolska 29, tel. (061) 832 48 94, tel./fax (061) 832 48 75, biuro@infocam.com.pl

AVerMedia AVerDiGi EB1304 MD



- Rejestrator cyfrowy typu Stand Alone
- Kompresja obrazu **MPEG4**
- 4 wejścia kamer BNC
- Wyjście wizyjne composite BNC i **VGA**
- 1 wejście i 1 wyjście **audio** RCA
- Prędkość wyświetlania 100 kl./sek.
- Prędkość zapisu 100 kl./sek. (tryb QUAD), **50 kl./sek.** (tryb EACH)
- Rozdzielczość zapisu **720x576** (tryb EACH), 360x288 (tryb QUAD)
- **Programowa detekcja ruchu**
- Praca w trybie Duplex
- Obsługa 1 dysku twardego bez limitu pojemności
- Technologia pomijania uszkodzonych sektorów dysku
- Graficzne menu ekranowe w języku polskim
- Złącze **USB 2.0** do komunikacji z komputerem PC
- 4 wejścia alarmowe, 1 wyjście przekaźnikowe
- Brak ruchomych elementów chłodzących
- Pilot zdalnego sterowania
- Wymiary: 290 x 180 x 50 mm

729,00 zł

NEC AccuSync LCD93V

- Monitor kolorowy VGA LCD 19"
- Rozdzielczość nominalna 1280x1024
- Jasność nominalna 300 cd/m²
- Kontrast 700:1
- Kąt widzenia 160° H x 160° V
- Czas reakcji plamki 8 ms
- 16,2 mln kolorów
- Waga 5,3 kg
- Wymiary (szer. x wys. x głęb.) 406 x 405 x 205 mm
- Zasilanie 230VAC

750,00 zł

AverDiGi TV2VGA

- Konwerter sygnału VGA na composite BNC
- Zakres rozdzielczości od 640x480 do1280x1024
- Maksymalna częstotliwość wyświetlania 85Hz
- Przelotowe wejście wideo BNC
- Przelotowe wyjście VGA D-sub 15 pin
- Regulacja kontrastu, jasności, nasycenia, barwy
- Menu ekranowe OSD
- Funkcja elektronicznej redukcji szumów NRF
- Zasilacz 5VDC w zestawie

235,00 zł

NeoTech J2000S-16T1CUV

- Rejestrator cyfrowy typu Stand Alone
- 16 przelotowych wejść kamer
- Prędkość wyświetlania **400 kl./sek.**
- Zapis obrazu z prędkością **100 kl./sek.** w rozdzielczości **720x288**, 200 kl./sek. w rozdzielczości 360x280
- Algorytm kompresji **JPEG2000** (wysoka jakość zapisanego obrazu, mały rozmiar pliku)
- Praca w trybie **Triplex** (Odtwarzanie, Nagrywanie, Praca w sieci)
- Zdalny podgląd obrazu dobrej jakości przez TCP/IP (obsługa **DDNS**)
- Automatyczne wykrywanie ustawień sieciowych DHCP
- Wbudowane wyjście **VGA** (obsługa monitorów TFT LCD)
- Backup danych poprzez wbudowaną nagrywarkę **CD-RW** lub port **USB 2.0**
- Programowa detekcja ruchu
- Menu ekranowe w języku polskim
- Obsługa 1 dysku twardego bez limitu pojemności
- Pilot zdalnego sterowania
- Możliwość podłączenia pulpitu sterującego J2000-KB485

3 995,00 zł

3 150,00 zł NeoTech J2000S-08T1CUV - 8ch

Zestaw obserwacyjny

- Rejestrator cyfrowy **AVerDiGi EB1304 NET** (kompresja MPEG4, praca w sieci LAN, wyjście VGA, 4ch video, 1ch audio, 100kl./sek., rozdz. 720x576, detekcja ruchu, USB 2.0)
- Dysk twardy **320GB**
- Kolorowy monitor LCD 17" **NEC 73V**
- 4 x kamera kolorowa typu **CAMSTAR CAM-412D** (1/3" Sony Super HAD; 420 linii TV; 0,5 luxa przy F 1.2; wbudowany obiektyw 3.6 mm)

3 499,00 zł

AVerMedia AVerDiGi NV5000

- Karta PCI + oprogramowanie w języku polskim
- Praca w systemach operacyjnych Windows 2000 / XP
- Maksymalna rozdzielczość wyświetlania i zapisu 720x576
- Kompresja obrazu advanced MPEG-4
- Funkcja deinterlacji graficznej zwiększająca jakość obrazu
- Funkcja automatycznej redukcji szumów NRF
- Wbudowane wyjście TV-OUT
- Cyfrowy zoom obrazu w podglądzie „na żywo" i w archiwum
- Praca w sieci LAN, WAN, ISDN, SDI, ADSL
- Tryb pełnoekranowy w podglądzie i archiwum
- Wyszukiwanie archiwum po dacie, czasie, zdarzeniach alarmowych, detekcji ruchu, inne
- Transmisja na odległość (WebCam, zdalna konsola, PDA, GSM, Centrum)
- Obsługa dynamicznych nazw domen DDNS
- Możliwość zdalnej zmiany ustawień i podglądu archiwum
- Programowa detekcja ruchu z możliwością ustawienia masek detekcji
- Funkcja inteligentnego i wizualnego wyszukiwania zdarzeń
- Wizualizacja operacji kasowych POS
- Znak wodny i 5 poziomów zabezpieczeń hasłami
- Możliwość rejestracji dźwięku (dodatkowe rozszerzenia)
- Nowe oprogramowanie ver. 7.1

NV5004
Karta PCI, 4 wejścia wideo
Wyświetlanie/Nagrywanie: 100 kl./sek.
Możliwość łączenia w system 8ch 200kl./sek.

1 599,00 zł

NV5008 / 100
Karta PCI + rozszerzenie, 8 wejść wideo
Wyświetlanie / Nagrywanie: 100 kl./sek.

1 749,00 zł

NV5016 / 100
Karta PCI + 3 rozszerzenia, 16 wejść wideo
Wyświetlanie / Nagrywanie: 100 kl./sek.

2 049,00 zł

NV5016 / 200
2 karty PCI + 2 rozszerzenia, 16 wejść wideo
Wyświetlanie / Nagrywanie: 200 kl./sek.

3 450,00 zł

CAMSTAR CAM-612DV3

- Kamera kolorowa typu Dome
- Obudowa hermetyczna, **wandaloodporna**
- Wbudowany promiennik podczerwieni IR 12 diód, zasięg 10 m
- Przetwornik 1/3" **Sony** Super HAD
- Rozdzielczość **480 linii TV**
- Czułość 0 luxa przy aktywnych diodach IR
- Wbudowany obiektyw 3.6 mm
- Automatyczna kompensacja tylnego światła
- Automatyczny balans bieli
- Zasilanie 12VDC
- Wymiary ϕ 94 x 80 mm

415,00 zł

Zestaw zewnętrzny

- Kamera kolorowa typu Dzień/Noc SW CAM SCC-13S (1/3" Sony Super HAD, 540 linii TV, 0.002 luxa przy F1.2, menu ekranowe OSD, funkcja Sens Up, DNR, maski prywatności)
- Obiektyw szklany z AutoIris DC 2,8-12 mm ZS 2812A
- Obudowa zewnętrzna z grzałką i uchwytem GL-606H

785,00 zł

Podane ceny nie zawierają podatku VAT 22%.
Oferta promocyjna obowiązuje do wyczerpania zapasów.
Niniejsza oferta nie stanowi oferty handlowej w rozumieniu art. 66 par. 1 KC oraz innych właściwych przepisów prawnych.

artykuł sponsorowany

exacqVision

– hybrydowy system nadzoru wizyjnego do kamer analogowych i kamer IP

exacqVision jest najnowocześniejszym rozwiązaniem cyfrowej telewizji dozorowej. System został zaprojektowany jako wspólna platforma do najnowszych kamer IP oraz tradycyjnych kamer analogowych. Jednolity, niezwykle intuicyjny interfejs użytkownika wygląda tak samo zarówno w przypadku małych instalacji i rozległych systemów z dużą liczbą kamer. Pozwala to na swobodną ewolucję od tradycyjnych kamer analogowych do systemów wykorzystujących technologię IP, bez konieczności rezygnowania z istniejącej infrastruktury. Technologia exacqVision pozwala łączyć w jednym systemie wszystkie typy kamer CCTV: analogowe, IP, o rozdzielczości standardowej i megapikselowej, stacjonarne, na głowicach PTZ, szybkoobrotowe, wykorzystujące różne formaty kompresji

Budowa systemu

System exacqVision został zbudowany z wykorzystaniem stabilnej i bezpiecznej architektury klient/serwer. Podstawowym elementem, odpowiadającym za rejestrację i analizę obrazu oraz jego przechowywanie i udostępnianie, jest serwer exacqVision (exacqVision Server). Dostępne są wersje hybrydowe – do kamer analogowych i kamer IP, oraz wyłącznie do kamer IP. Obsługa, zarządzanie kamerami, strojenie i programowanie systemu, podgląd obrazu, odsłuch dźwięku, eksport i archiwizacja nagrań odbywa się za pomocą oprogramowania exacqVision Client. Komunikacja pomiędzy klientami i serwerami odbywa się poprzez sieć LAN/WAN z wykorzystaniem protokołów TCP/IP.

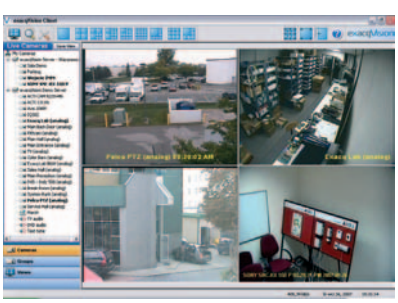
Do serwera exacqVision może być podłączonych jednocześnie wiele klientów. Jeden klient exacqVision może być podłączony w tym samym czasie do wielu serwerów exacqVision. Tworzy to rozległy system klasy Enterprise.

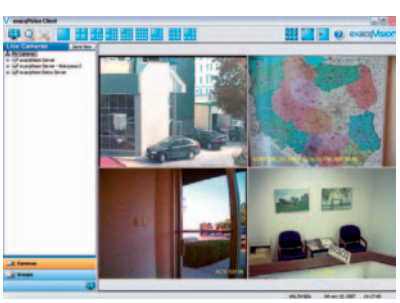
Elementy systemu

SERWERY HYBRYDOWE (kamery analogowe oraz IP)

exacqVision Pro jest hybrydowym rozwiązaniem do zapisu i zarządzania obrazem pozwalającym łączyć w jeden system rozwiązania tradycyjnych kamer analogowych z najnowszą technologią kamer IP. Specjalnie zaprojektowana, nowoczesna obudowa Rack 2U umożliwia podłączenie do 64 kamer, w tym 32 kamer analogowych i (lub) do 64 kamer IP. Niewielkie rozmiary i zoptymalizowane chłodzenie umożliwiają bezpieczną pracę i zaoszczędzenie cennego miejsca w szafach. Dostępna jest również wersja RAID 5.

Do kompresji obrazu z kamer analogowych wykorzystywane są dedykowane układy elektroniczne. Dzięki temu obciążenie głównego procesora serwera nie przekracza kilku procent, pozwalając wykorzystać wolną moc obliczeniową do integracji z innymi systemami, np. BMS, systemami





zabezpieczeń, bankomatami czy kasami fiskalnymi. Nowoczesny standard kompresji obrazu MPEG-4 ASP gwarantuje wysoką jakość obrazu przy stosunkowo najmniejszym rozmiarze materiału archiwalnego. Możliwość nagrywania do 800 obrazów na sekundę, rozdzielczość D1 (4CIF), trzy wyjścia wideo, licencja ośmiu kamer IP w cenie systemu to tylko niektóre zalety zwiększające jego atrakcyjność.

SERWERY IP (kamery i wideoserwery IP)

exacqVision IP rozszerza platformę exacqVision poprzez udostępnienie systemów kamer IP wykorzystujących ten sam nowoczesny i intuicyjny interfejs użytkownika. Dostępny wyłącznie jako oprogramowanie bądź jako zoptymalizowany serwer, exacqVision IP jest najprostszym w obsłudze i konfiguracji systemem monitoringu CCTV/IP. exacqVision IP jest bardzo wygodny w dystrybucji: cechuje go stała, niska cena za kanał wideo i nieskomplikowany, wykorzystujący adresy MAC schemat licencjonowania. exacqVision IP przełamuje mity związane ze złożonością projektowania i implementacji systemów zapisu i zarządzania obrazem CCTV/IP.

KLIENT

Klient exacqVision ma identyczną funkcjonalność i interfejs we wszystkich systemach exacqVision. Można dowolnie mieszać i łączyć systemy exacqVision IP oraz exacqVision Pro w celu połączenia kamer IP oraz analogowych w jeden hybrydowy i skalowalny system zarządzania i zapisu obrazu. Pełna obsługa systemu realizowana jest za pomocą oprogramowania exacqVision Client, instalowanego w dedykowanych stacjach roboczych. Wspólny interfejs użytkownika dla oprogramowania klienckiego, instalowanego zarówno w przypadku serwerów i klientów, nie jest trudny w obsłudze, co upraszcza posługiwanie się systemem.

System prawdziwie hybrydowy

System exacqVision obsługuje w ten sam sposób obraz i dźwięk z kamer analogowych i kamer IP. Pozwala to wykorzystać istniejącą sieć Ethernet oraz infrastrukturę obiektu (kable i kamery analogowe). Do pojedynczego serwera exacqVision można podłączyć maksymalnie 64 kamery. Kamery analogowe można podłączać również poprzez wideoserwery IP. Dzięki wykorzystaniu serwerów hybrydowych exacqVision Pro, serwerów exacqVision IP oraz wideoserwerów IP istnieje możliwość dowolnego projektowania rozwiązań cyfrowego monitoringu wizyjnego oraz dopasowania takiej konfiguracji, jaka wynika z architektury obiektu, a nie z ograniczeń systemów analogowych.

Wirtualna krosownica

Sieć serwerów (rejestratorów) tworzy system monitoringu wizyjnego, który jest zintegrowany ze zdecentralizowanymi stanowiskami nadzoru w dowolnym punkcie sieci LAN/WAN bez dodatkowych opłat.

System exacqVision umożliwia wykonywanie wszystkich funkcji typowych dla tradycyjnej krosownicy wizyjnej, a ponadto, dzięki technologii cyfrowej, wiele funkcji niedostępnych w technologii analogowej. Do jednej stacji roboczej można dołączyć kilka monitorów i wyświetlać obraz z różnych kamer oraz jednocześnie odtwarzać czy zmieniać ustawienia serwera. Inne możliwości systemu to: wyświetlanie obrazu z kamer z różnych serwerów, dowolne widoki (podział ekranu wg ustawień operatora) i sekwencje widoków, monitory alarmowe, tworzenie relacji logicznych w celu wyświetlenia określonego widoku (np.: detekcja ruchu na kamerze nr 8 powoduje wyświetlenie widoku Piętro 1 na monitorze 1 oraz kamery 8 na monitorze 2). Dodatkowym efektem wykorzystania funkcji wirtualnej krosownicy jest monitorowanie zdarzeń. Dzięki niemu operator może potwierdzać docierające do centrum nadzoru zdarzenia oraz przełączać się na widok z danej kamery wprost z okna rejestru zdarzeń.

Detekcja ruchu, wejścia alarmowe

System exacqVision ma funkcję detekcji ruchu, która jest ustawiana dla każdej kamery niezależnie. Wielkość wykrywanego obiektu oraz czułość detekcji można regulować. Każdy serwer hybrydowy posiada wejścia i wyjścia alarmowe. W ten sam sposób można wykorzystywać wejścia i wyjścia dostępne w kamerach i wideoserwerach IP.

PTZ i porty szeregowe

System exacqVision zapewnia obsługę analogowych głowic PTZ, a także kamer PTZ/IP. W ten sam sposób można obsługiwać funkcję Digital PTZ, czyli także cyfrowy zoom, co jest szczególnie istotne w przypadku zainstalowania kamer megapikselowych. System umożliwia definiowanie pozycji (presetów) dla wszystkich typów kamer oraz wykorzystanie tzw. presetów cyfrowych, czyli ustawialnych zbliżeń cyfrowych. Wszystkie presety mogą być również wywoływane automatycznie, w reakcji na zdarzenia. Możliwa jest obsługa za pomocą myszy lub joysticka USB.

exacqVision można zintegrować z dowolnym systemem POS (kasy fiskalne), ATM (bankomaty) lub innym wykorzystującym porty szeregowe. Zapewniono kompleksowy interfejs obsługi tekstu kojarzonego z obrazem, a także obsługę wyszukiwania poszczególnych informacji z paragonów lub bankomatów.

Zdarzenia

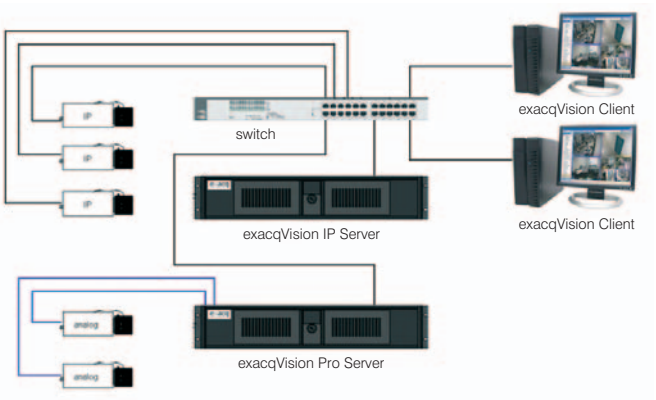
Poza standardowymi trybami nagrywania obrazu, takimi jak harmonogramy, detekcja ruchu, zapis ciągły czy zapis poklatkowy, w exacqVision udostępniono także system obsługi zdarzeń. Źródłem zdarzeń mogą być: informacje uzyskane z detekcji ruchu lub z wejścia alarmowego, zanik obrazu, informacja z kasy fiskalnej lub dowolna inna z portu szeregowego, brak połączenia z kamerą IP, informacje diagnostyczne z serwera, zbyt wysoka temperatura albo awaria systemu RAID. W reakcji na zdarzenia można uruchomić nagrywanie obrazu ze zdefiniowanymi parametrami, nagrywanie dźwięku z dowolnego mikrofonu, zmienić stan wyjścia alarmowego, wywołać obraz na wyjściu alarmowym, ustawić kamerę szybkoobrotową w odpowiedniej, zdefiniowanej wcześniej pozycji, wysłać email z powiadomieniem o zdarzeniu, nagrać materiał na płytę DVD. Wszystkie zdarzenia dotyczące nagrywania mogą mieć zdefiniowany czas przed alarmem oraz po alarmie.

Obsługa kamer analogowych

Zaawansowana kompresja MPEG-4 ASP umożliwia przechwytywanie obrazu w czasie rzeczywistym ze znakowaniem (*watermarking*) dla każdej kamery. Do jednego serwera można podłączyć do 32 kamer analogowych. Parametry każdej kamery, takie jak gęstość zapisu, rodzaj zapisu, maska prywatności, detekcja ruchu, rodzaj i stopień kompresji, są ustawianie indywidualnie.

Obsługa kamer IP

Każdy serwer exacqVision może obsłużyć, jak wspomniano, do 64 kamer IP. W jednym serwerze mogą funkcjonować kamery IP różnych producentów. Do wyszukiwania kamer w sieci oraz ustawienia ich parametrów nie jest wymagane oprogramowanie producenta. System exacqVision obsługuje wszystkie rodzaje kompresji oraz rozdzielczości, w tym megapikselowe, udostępniane przez dostawców kamer. Obecnie jest kompatybilny z kamerami IP oraz wideoserwerami następujących producentów: Axis, Sony, IQinVision, ACTI, Arecont Vision, Panasonic, CBC, Vivotek, GE Security, Armida Technologies. Wkrótce obsługiwane będą również urządzenia Sanyo, PiXORD, Mobotix, Pelco oraz ioimage. Aktualna lista dostępna jest na stronie www.exacq.pl.



Zapis dźwięku

System exacqVision umożliwia zapis dźwięku zarówno z wejść mikrofonowych w serwerach analogowych exacqVision Pro, jak również z wejść, dostępnych w kamerach i wideoserwerach IP. Parametry nagrywanego dźwięku umożliwiają wykorzystanie systemu do obsługi imprez masowych zgodnie z polskimi przepisami.

Skalowalność

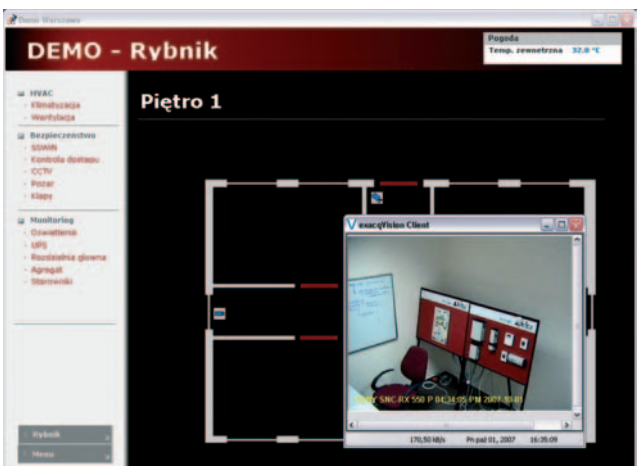
System exacqVision ma budowę modułową. Nie ma limitu w zakresie liczby jednocześnie pracujących w sieci serwerów, a także klienckich stacji roboczych. W ramach jednego serwera można zamawiać licencje na określoną liczbę kamer IP – nie trzeba płacić za niewykorzystane zasoby.

Funkcjonalność

Interfejs użytkownika w systemie exacqVision jest bardzo przyjazny oraz intuicyjny. Przy **podglądzie obrazu** można wyłączyć wszystkie ramki i menu, pozostawiając na monitorach wyłącznie obrazy z kamer. System automatycznie wykrywa rozdzielczość monitorów i udostępnia układy kamer 4x5 czy 5x6 w proporcji 16:9. Dowolnie definiowane widoki użytkownika umożliwiają szybką reakcję operatorów na zdarzenia zachodzące w systemie. Dodatkowo można zautomatyzować przełączanie obrazu w reakcji na detekcję ruchu, zdarzenie czy informację z zewnętrznych systemów. Dostępne są funkcje grupowania kamer według ich rzeczywistej lokalizacji, a nie według podłączenia do rejestratorów. Ciekawa jest funkcja exacqReplay, umożliwiająca szybką powtórkę z ostatniej chwili (do pięciu minut wstecz).

W zakresie **odtwarzania i wyszukiwania obrazu** system exacqVision oferuje wiele opcji konfiguracyjnych. Można określić parametry czasowe i ograniczyć poszukiwania do obrazów z określonych kamer lub zdarzeń. Fizyczna lokalizacja kamer jest nieistotna z punktu widzenia operatora. Po prostu określamy zakres poszukiwań, a w odpowiedzi otrzymujemy graficzną reprezentację wyników. Funkcja ta zdecydowanie ułatwia poruszanie się w systemach z większą liczbą kamer. Dodatkowo dostępna jest opcja SmartSearch, tzw. wtórna detekcja ruchu, czyli analiza obrazu nagranego niezależnie od ustawień systemowej detekcji ruchu w czasie rzeczywistym.

Administrowanie systemem odbywa się z tego samego oprogramowania exacqVision Client. W zależności od



uprawnień zalogowany użytkownik może zdalnie lub lokalnie zmieniać wszystkie ustawienia i parametry systemu. Oprogramowanie konfiguracyjne instalowane na serwerach jest identyczne z tym w stacjach roboczych. Dzięki takiemu rozwiązaniu możliwe jest całkowite uniezależnienie operatora od fizycznej lokalizacji rejestratorów.

Bezpieczeństwo

System exacqVision wykorzystuje bezpieczną architekturę klient/serwer. Korzysta z wbudowanych mechanizmów autoryzacji, dostępnych w systemach operacyjnych. Poza tym komunikacja pomiędzy klientem i serwerem jest szyfrowana. W systemie wykorzystywana jest wielopoziomowa struktura uprawnień, która umożliwia ograniczenie dostępu do wielu ustawień oraz poszczególnych kamer.

Podsumowanie

Stabilna architektura systemu, wykorzystanie nowoczesnej technologii informatycznej oraz dynamiczny rozwój produktu gwarantują dostosowanie systemu exacqVision do najnowszych standardów telewizji dozorowej. Otwarty interfejs programowania aplikacji (API – ang.: Application Programming Interface) pozwala zintegrować system exacqVision z innymi systemami (BMS, kontrola dostępu, systemy alarmowe, bankomaty, kasy fiskalne i inne). Co sześć tygodni inżynierowie firmy Exacq Technologies opracowują nowe funkcje, które można z łatwością implementować w istniejących systemach, podnosząc w ten sposób ich funkcjonalność. Więcej informacji znajdziecie Państwo na stronie www.exacq.pl lub w biurach handlowych firmy Delta Controls.

Jarosław Tężycki
DELTA CONTROLS

Rejestrator Novus serii 5000 – nowa generacja

Rejestratory firmy Novus serii 5000 były szczegółowo opisywane na łamach *Zabezpieczeń* w numerze 6/2005. W kolejnych wydaniach zostały przedstawione cechy funkcjonalne aplikacji sieciowych RAS/RAS+ oraz modułów do tworzenia podkładów graficznych (map). Oferta rejestratorów serii 5000 zostanie rozszerzona o 16-kanałowy model o nazwie NV-DVR5816/DVD, który będzie obsługiwany zdalnie, również z poziomu aplikacji RAS+, i będzie posiadał wiele nowych funkcji. Właśnie tym nowym, wyróżniającym funkcjom chciałbym poświęcić niniejszy artykuł.

Rejestrator NV-DVR5816/DVD zapisuje obrazy z kamer w czasie rzeczywistym (ang. *real time*) z prędkością 25 klatek na sekundę dla każdego kanału, czyli 400 klatek na sekundę dla całego systemu. Rejestracja ta jest realizowana w rozdzielczości HALF D1 720x288, jak w poprzednich modelach serii. Dodatkowo istnieje możliwość rejestracji w rozdzielczość D1 720x576, z prędkością o połowę mniejszą, czyli 200 klatek na sekundę dla wszystkich kanałów. W celu uniknięcia rozmazywania szybko przemieszczających się obiektów między dwoma kolejnymi półobrazami podczas odtwarzania obrazów zarejestrowanych w rozdzielczości D1 zaimplementowano funkcję deinterlacingu, niwelującą to niekorzystne zjawisko.

Rejestrator spełnia wymagania zawarte w *Rozporządzeniu w sprawie sposobu utrwalania przebiegu imprez masowych oraz minimalnych wymagań technicznych dla urządzeń rejestrujących obraz i dźwięk z dnia 28 października 2004 r. (Dz. U. z 2004 r., nr 243, poz. 2438),* co jest szczególnie ważne w kontekście planowanej budowy obiektów sportowych w związku z organizowaniem wspólnie z Ukrainą mistrzostw Europy w piłce nożnej. W § 5 powyższego rozporządzenia zawarte są wymagania, zgodnie z którymi „urządzenia utrwalające obraz powinny rejestrować obraz z częstotliwością 25 klatek na sekundę dla każdej kamery, z rozdzielczością nie mniejszą niż 400 linii telewizyjnych".

W urządzeniu można zainstalować maksymalnie cztery dyski twarde z interfejsem SATA, o pojemności 500 GB każdy, w wyjmowanych kieszeniach. Wymiana twardych dysków może być realizowana bez wyłączania urządzenia z sieci zasilającej (dyski typu *hot-swap*). Dodatkowo poprzez złącze SCSI można podłączyć zewnętrzne macierze dyskowe. Urządzenie może zaadresować łącznie do 9 TB pamięci wewnętrznej i zewnętrznej. W rejestratorze zaimplementowano system kompresji MPEG4. Przy najwyższej jakości oraz rozdzielczości D1 pojedyncza zarejestrowana klatka posiada rozmiar pliku osiągający nawet 80 kB, co gwarantuje dużą rozpoznawalność szczegółów. W rejestratorze zaimplementowano zmienny system kompresji VBR (*Variable Bit Rate*) generujący różne rozmiary pojedynczej klatki w zależności od rodzaju obserwowanej sceny. Do zabezpieczenia rejestrowanych danych można wykorzystać nie tylko funkcję archiwizacji, czyli kopiowania na wybrany dysk rejestrowanych danych, ale także funkcję mirroringu (zapis lustrzany w pamięciach dyskowych, w wyniku którego dwa napędy dyskowe przechowują taką samą informację). Funkcja archiwizacji, w przeciwieństwie do mirroringu, ma niższy priorytet w stosunku do procesu archiwizacji, odtwarzania oraz transmisji sieciowej i jest realizowana wówczas, gdy istnieją wolne zasoby systemowe. Natomiast funkcja mirroringu jest realizowana w czasie rzeczywistym, bez opóźnień. Możliwe jest ustalenie poziomu jakości obrazów transmitowanych przez sieć i nie ma on wpływu na jakość zapisu oraz rozdzielczości obrazów odtwarzanych zdalnie (CIF, 2 CIF).

Urządzenie zostało wyposażone w 16 wejść audio oraz jedno wyjście głośnikowe, czyli z każdym kanałem wizji ➡

NOVUS®

Profesjonalne rozwiązanie dla systemów CCTV

NOWA seria IR

obiektywy z przysłoną automatyczną

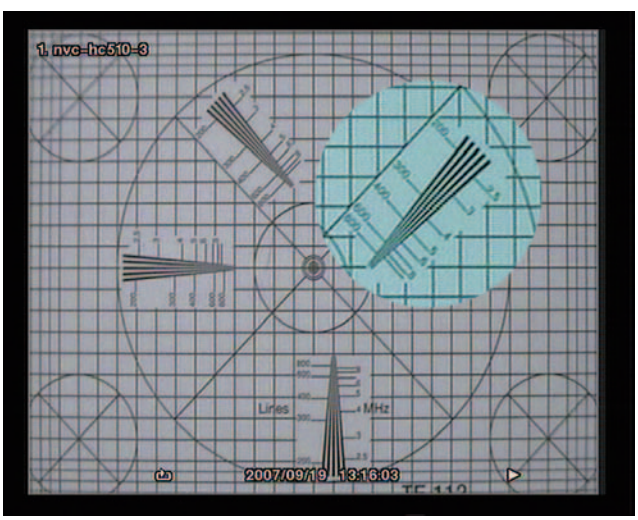
- o dużej jasności (od F1.0)
- dedykowane do kamer typu dzień/noc oraz kamer współpracujących z promiennikami podczerwieni
- asferyczne soczewki wykonane ze szkła ED o bardzo niskim współczynniku rozpraszania światła
- niwelują zjawiska aberracji chromatycznej i sferycznej

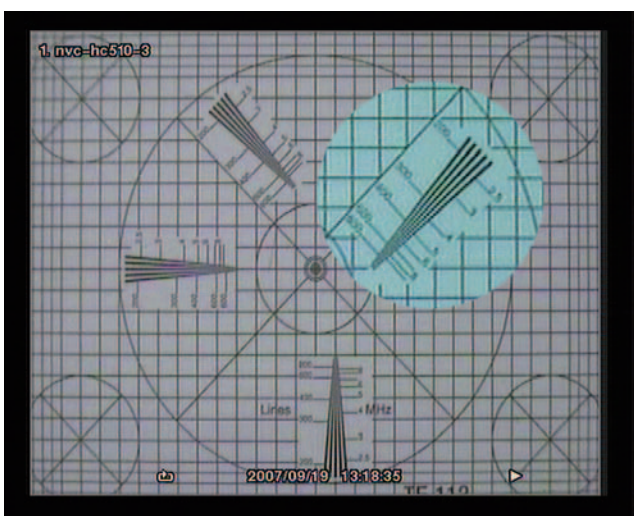
Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

może zostać skojarzony oddzielny kanał fonii. Kanały fonii są rejestrowane i mogą być odtwarzane synchronicznie z odpowiednimi kanałami wizji. Dotyczy to również materiałów skopiowanych lokalnie na pamięci typu USB Flash lub nośniki DVD, a także przez sieć. Poprzez sieć, za pomocą aplikacji RAS+ lub dzięki przeglądarce internetowej, możliwa jest transmisja dowolnego, wybranego przez operatora kanału audio. Dodatkowo operator może zdalnie przesłać dźwięk do podłączonego do rejestratora głośnika.

Ustawienia funkcji utraty obrazu zostały zindywidualizowane dla każdej kamery (w dotychczasowych modelach ustawienie to było globalne i dotyczyło wszystkich kamer w systemie). Dzięki temu są precyzyjne i umożliwiają otrzymywanie wiarygodnych powiadomień o zasłonięciu obiektywu, jego zamalowaniu lub przesunięciu kamery. W wymienionych sytuacjach kamera działa prawidłowo, generuje odpowiedni dla obserwowanej sceny sygnał wizyjny, ale jego wartość informacyjna dla operatora systemu jest zerowa, dlatego otrzymanie odpowiedniego powiadomienia pozwala na szybką reakcję administratora i przywrócenie sprawności systemu.





Rys. 1. Tablica testowa rozdzielczości zarejestrowanych obrazów z kamery NVC-HC510-3 dla rozdzielczości 720x288 (420 TVL) oraz 720x576 (450 TVL)

Oprócz funkcji detekcji ruchu, z różnymi parametrami dla dnia oraz nocy, zaimplementowano funkcję detekcji obiektu w czasie rzeczywistym. Po zapisaniu obrazu referencyjnego dla systemu oraz ustaleniu minimalnego czasu analizy system potrafi powiadomić o pozostawionych w miejscach publicznych walizkach, otwartych drzwiach czy pojawieniu się lub zniknięciu innych dowolnych obiektów. Funkcja ta może być szczególnie przydatna w obiektach użyteczności publicznej, np. na dworcach lotniczych lub kolejowych.

Dla materiału zarejestrowanego wprowadzono znaczniki (*bookmarks*), umożliwiające intuicyjne zaznaczanie dowolnych pozycji i łatwy do nich dostęp. Są one przydatne również podczas zaznaczania początku i końca czasu kopiowania – można posłużyć się znacznikami, zamiast wpisywać datę i czas.

W przypadku powiadamiania o zdarzeniach krytycznych poprzez e-mail istnieje możliwość dołączania do wiadomości pojedynczej klatki zarejestrowanego obrazu powiązanego ze zdarzeniem.

Monitor główny można podłączyć do rejestratora poprzez złącze BNC, VGA lub S-Video. Wszystkie te trzy wyjścia mogą pracować jednocześnie. Rozdzielczość wyświetlania 800x600 i częstotliwość odswieżania 60 Hz na wyjściu zostały dopasowane do parametrów technicznych monitorów VGA dostępnych na rynku. Na monitorze głównym można równocześnie odtwarzać obraz z kamery i dokonywać podglądu na żywo – w dowolnie wybranym podziale.

Spośród szesnastu wyjść alarmowych dwanaście to wyjścia typu otwarty kolektor, natomiast cztery są wyjściami przekaźnikowymi o maksymalnym obciążeniu 30 VDC/1 A. Aby ułatwić podłączanie zewnętrznych urządzeń, takich jak kamery obrotowe, klawiatury lub urządzenia generujące dane tekstowe, w urządzenie wbudowano dwa porty RS485 i dwa porty RS232.

W rejestratorze zamontowany jest ciekłokrystaliczny wyświetlacz, na którym wyświetlane są informacje o realizowanych procesach, m.in. o temperaturze twardych dysków, zalogowanych do systemu użytkownikach, zajętości twardego dysku, aktywacji alarmu, aktualizacji firmware'u, nagrywania itp.

Rejestrator NV-DVR5816, podobnie jak inne modele serii 5000, może być programowany całkowicie za pomocą aplikacji RAS+. Ponadto może być sterowany lokalnie, za pomocą przycisków panelu czołowego, pilota zdalnego sterowania IR, klawiatury systemowej NV-KBD60 lub NV-KBD30, a także myszy komputerowej z interfejsem USB. Niezależnie od sposobu sterowania dostęp do funkcji rejestratora jest chroniony jednolitym systemem haseł oraz poziomów dostępu ustawianych w menu.

Rejestrator pracuje w trybie pełnego pentaplexu, tzn. pozwala na jednoczesne nagrywanie, podgląd na żywo, odtwarzanie, transmisję sieciową oraz mirroring/archiwizację zarejestrowanych danych.

Rejestrator NV-DVR5816 należy do rejestratorów o najlepszych parametrach technicznych wśród dostępnych na rynku. Co bardzo ważne, „dziedziczy" najważniejsze zalety serii 5000: wysoką stabilność i bezawaryjność ciągłej pracy. W połączeniu z rozbudowanymi funkcjami monitoringu procesów rejestratora i funkcjami powiadamiania m.in. do pięciu zdalnych aplikacji z uruchomioną aplikacją RAS+ oraz poprzez e-mail umożliwia to stosowanie urządzenia w obiektach o najwyższych wymaganiach dotyczących bezpieczeństwa.

Patryk Gańko
Novus

Analogowy adresowalny system sygnalizacji pożarowej Panasonic EBL512

System sygnalizacji pożarowej EBL512 jest produktem firmy Panasonic Electric Works Fire&Security Technology Europe, którego dystrybutorem na polskim rynku jest firma RAJ International. Japoński producent zabezpieczeń przeciwpożarowych jest obecny na naszym rynku od kilkunastu lat i **jako pierwszy zaoferował analogowy system wykrywania pożaru EBL2000**, którego następcą jest analogowy system EBL1000. System Panasonic EBL512 jest najnowszym produktem, przeznaczonym do ochrony obiektów średnich i dużych, charakteryzujących się dużym zróżnicowaniem technicznym.

Centrala EBL512 jest mikroprocesorową centralą systemu sygnalizacji pożarowej, przeznaczoną do współpracy z analogowymi, adresowalnymi czujkami dymu, czujkami konwencjonalnymi, ręcznymi ostrzegaczami pożarowymi, modułami sterującymi. Każda centrala umożliwia podłączenie czterech pętli z czujkami, przyciskami ROP oraz elementami wejścia/wyjścia dla funkcji dowolnie programowanych pod kątem określonego obiektu lub innych rodzajów urządzeń. W przypadku, gdy liczba 512 adresów dla elementów liniowych jest niewystarczająca, EBL512 umożliwia łączenie w sieć do 30 central, co zwiększa pojemność systemu do ponad 15000 elementów liniowych. Centrale komunikują się pomiędzy sobą za pomocą sieci TLON. Każda z central w sieci posiada dostęp do wszystkich informacji z innych central znajdujących się w tej samej sieci – są one równorzędne. Nowością na rynku systemów sygnalizacji pożarowej jest możliwość monitorowania stanu systemu Panasonic EBL512 praktycznie z dowolnego miejsca na świecie. Zastosowanie modułu Web Server 1598 umożliwia, za pomocą Internetu lub sieci LAN, uzyskanie informacji o alarmach pożarowych, alarmach serwisowych (np. wówczas, kiedy czujki są zabrudzone), uszkodzeniach, zblokowanych strefach lub poszczególnych elementach systemu. Moduł umożliwia także wysyłanie informacji o stanie systemu na cztery zaprogramowane adresy e-mail.

Bardzo mocną stroną systemu Panasonic EBL512 są elementy detekcyjne. Podczas jego projektowania postawiono sobie za cel maksymalne zwiększenie skuteczności wykrywania pożaru przy jednoczesnej minimalizacji fałszywych alarmów. Z centralą EBL 512 współpracują analogowe, adresowalne optyczne czujki dymu, termiczne czujki dymu oraz zaawansowane technicznie multisensory, łączące zalety czujki termicznej i optycznej. Alarm pożarowy jest sygnalizowany przez każdą czujkę w systemie indywidualnie. Podczas alarmu strefa i adres czujki wykrywającej pożar (tzw. numer prezentacyjny) pokazywane są na wyświetlaczu płyty czołowej centrali wraz z 40-znakowym dowolnym opisem. Pozwala to, w połączeniu z planem rozmieszczenia czujek, na zlokalizowanie miejsca pożaru w możliwie najkrótszym czasie.

Każda centrala monitoruje elementy podłączone do swoich pętli dozorowych co 2,5 sekundy. Co trzy minuty następuje zmiana kierunku dozorowania w pętli komunikacyjnej. Umożliwia to szybkie wykrycie przerwy pomiędzy centralą a pierwszym lub ostatnim elementem w pętli komunikacyjnej.

Zastosowane czujki analogowe adaptują się do warunków otoczenia, w jakich pracują. Zapobiega to generowaniu fałszywych alarmów z powodu postępującego zabrudzania się komór pomiarowych w czujkach. Procesor centrali oblicza poziom odniesienia indywidualnie dla każdej czujki i powyżej tego progu ustala, według zaprogramowanego algorytmu, próg alarmu pożarowego. Centrala EBL512 odczytuje co około 2,5 sekundy wartość chwilową każdej czujki. Wskazanie to jest proporcjonalne do warunków panujących wokół niej. W celu utrzymania stałej czułości pracy każdej czujki, poziom odniesienia każdej z nich jest obliczany indywidualnie, jako średnia arytmetyczna z zapamiętanych

wartości chwilowych, odczytywanych co jedną godzinę w ciągu tygodnia. Umożliwia to zastosowanie systemu w najtrudniejszych nawet warunkach otoczenia. W przypadku przekroczenia przez poziom odniesienia progu alarmu serwisowego, zabrudzenie czujki jest sygnalizowane przez zaświecenie się żółtej diody LED, opisanej jako „Alarm serwisowy" na panelu kontrolnym centrali. Numer techniczny czujki będącej źródłem alarmu serwisowego i jej aktualny poziom odniesienia można odczytać na wyświetlaczu alfanumerycznym i wydrukować na drukarce w centrali pożarowej. Ponadto każda czujka:

– może być zaprogramowana na jeden z sześciu poziomów czułości, w zależności od środowiska, w którym pracuje,
– posługuje się algorytmem uniemożliwiającym zadziałanie spowodowane chwilowym (przypadkowym) zadymieniem,
– posługuje się algorytmem zwiększającym jej czułość w przypadku powolnego przyrostu zadymienia w jej otoczeniu (pożary tlewne),
– może być blokowana/odblokowana czasowo, przez zegar wewnętrzny centrali lub zewnętrzne urządzenie odliczające,
– może mieć automatycznie zmieniany próg czułości, w zależności od pory dnia czy obecności lub nieobecności personelu obsługującego.

Centrala EBL512 może sterować innymi systemami bądź określonymi urządzeniami. Sterowanie może być realizowane bezpośrednio przez centralę lub elementy WE/WY, zainstalowane w pętli komunikacyjnej (dozorowej). Centrala posiada w standardzie następujące wyjścia sterujące:

– cztery programowalne, nadzorowane wyjścia napięciowe, dedykowane sygnalizatorom akustyczno-optycznym (S0-S3),
– dwa przekaźnikowe wyjścia programowalne (R0-R1),
– cztery wejścia programowalne (J0-J3),
– dwa wyjścia zasilające 24 V_{DC},
– dwa nieprogramowane wyjścia przekaźnikowe do monitoringu alarmu pożarowego i uszkodzenia w systemie,

W przypadku konieczności użycia większej liczby wyjść sterujących, centralę można wyposażyć w dodatkowe pakiety sterujące typu 1581 (maksymalnie sześć szt.), o ośmiu stykach programowalnych NO lub NC.

Centrala EBL512 została wyposażona w bogaty zestaw funkcji programowych do tworzenia algorytmów sterujących urządzeniami zewnętrznymi.

Dla użytkowników już posiadających starsze systemy EBL1000 oraz EBL2000 dobrą wiadomością jest to, że centrala EBL512 jest w pełni kompatybilna z elementami liniowymi starszego typu. Dzięki temu poprzez wymianę starej centrali na nową użytkownik może dokonać modernizacji i zwiększenia pojemności starego systemu wykrywania pożaru. Nie trzeba demontować istniejących linii dozorowych, aby otrzymać nowoczesny produkt o nowych możliwościach użytkowych.

System EBL512 spełnia wymagania normy europejskiej EN-54 i wymagania krajowe. Jest dopuszczany do użytku w krajach Unii Europejskiej, Bliskiego i Dalekiego Wschodu, a od niedawna również w Australii.

Więcej informacji o systemie sygnalizacji pożaru Panasonic EBL512 oraz pomoc techniczną można uzyskać u polskiego dystrybutora systemu – w firmie Raj International (*http://www.raj-international.net*).

Rafał Rusiecki, Jacek Bańbura
Raj International
dystrybutor Panasonic Electric Works
Fire&Security Technology Europe

Oblicza RFID część 1.

Funkcjonując w świecie, w którym podstawową wartością jest informacja, jesteśmy zmuszeni do poszukiwania i stosowania technik automatycznej identyfikacji. Potrzeba automatycznej identyfikacji poszczególnych elementów systemów wymiany informacji uwarunkowana jest nie tylko koniecznością związaną *stricte* z funkcjonowaniem świata wirtualnego, ale także potrzebą zapewnienia bezpieczeństwa, czynnikami ekonomicznymi oraz dążeniem do uproszczeń i wygody

Istnieje wiele metod automatycznej identyfikacji, stosowanych w różnych obszarach ludzkiej działalności. Na ich rozwój oraz cechy funkcjonalne mają wpływ wymagania określone przez współczesne trendy systemów bezpieczeństwa i automatyzacji procesów. Pośród wielu znanych technik automatycznej identyfikacji swój renesans przeżywają technologie wykorzystujące transmisję radiową – RFID (ang. *Radio Frequency Identification*).

Technologia RFID jest dziś bardzo popularna i medialna. Uważa się, że stanowić będzie panaceum na wszystkie słabości systemów identyfikacji. Tworzona jest wokół niej otoczka mistycyzmu i uważa się ją za supernowoczesną technologię.

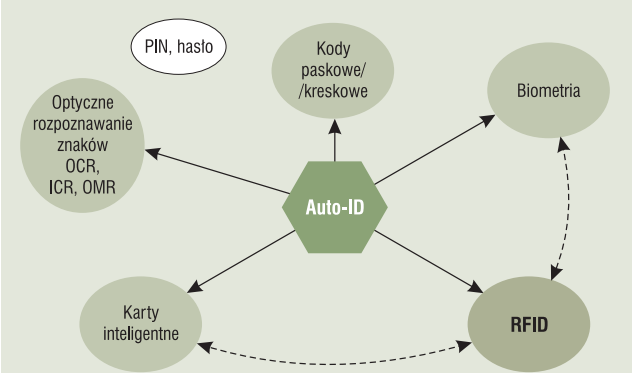
Czym jest RFID? Jakie niesie ze sobą korzyści i zagrożenia? Czy jest to technologia w pełni bezpieczna? – Odpowiedzi na te i szereg innych pytań postaram się udzielić w cyklu artykułów poświęconych temu tematowi.

A wszystko zaczęło się gdy…

W 1906 roku Ernst F. W. Alexanderson zademonstrował pierwszą falę ciągłą i transmisję sygnałów radiowych. To osiągnięcie dało początek nowoczesnej komunikacji radiowej.

Rok 1922 jest uważany za rok narodzin radaru, który wysyła fale radiowe w celu wykrywania i lokalizowania obiektu poprzez odbicie fal radiowych. W wyniku kombinacji technologii transmisji radiowej i radaru powstała koncepcja radiowej identyfikacji RFID. Pomysł zrodził się w umyśle naukowca Harry'ego Stockmana, prowadzącego w latach czterdziestych ubiegłego stulecia prace w zakresie komunikacji za pomocą odbitej mocy. Wkrótce pojawiły się pierwsze urządzenia wykorzystujące przemyślenia Stockmana, które pracowały na bazie wykrywacza metali.

Rys.1. Najbardziej znaczące procedury auto-ID



W latach pięćdziesiątych prowadzono prace związane z technologią RFID w zakresie systemu identyfikacji „przyjaciel czy wróg" (IFF – ang.: *identify friend or foe*) dla samolotów. W kolejnym dziesięcioleciu zaczęły już funkcjonować pierwsze sklepowe systemy antykradzieżowe, w których stosowano dekodowanie nalepki z obwodem rezonansowym lub systemy magnetoakustyczne wykorzystujące namagnesowane blaszki.

Był to okres wielu osiągnięć, które umożliwiły rozwój współczesnych systemów RFID. Warto wspomnieć m.in. o zdalnym aktywowaniu urządzeń za pomocą częstotliwości radiowych (Robert Richardson), komunikacji wiązką radarową (Otto Rittenback), biernych technikach transmisji danych wykorzystujących wiązkę radarową (J. H. Vogelman) oraz nasłuchująco-odpowiadającym systemie identyfikacji (J. P. Vinding).

Musiało minąć trzydzieści lat, zanim wizja Stockmana zaczęła się urzeczywistniać. Potrzebne były inne osiągnięcia: tranzystor, układ scalony, mikroprocesor, rozwój sieci komunikacyjnych, przemiany społeczne etc. Pełna identyfikacja radiowa pojawiła się w latach siedemdziesiątych, a pierwszym systemem ogólnie dostępnym był Tiris firmy Texas Instruments (*Texas Instruments Registration and Identification System*).

Producenci, wynalazcy, przedsiębiorstwa, instytucje uniwersyteckie i laboratoria rządowe aktywnie pracowały nad RFID. Znaczny postęp uzyskano między innymi w Los Alamos Scientific Laboratories, na Uniwersytecie Northwestern, czy w Microwave Institute Foundation w Szwecji. Wczesnym i ważnym osiągnięciem była praca zaprezentowana przez Alfreda Koelle, Stevena Deppa i Roberta Freymana *Telemetria o krótkim zasięgu do elektronicznej identyfikacji*, używająca modulowanego rozproszenia wstecznego z 1975 roku.

Technologię RFID rozwijały również duże koncerny, na przykład Raytheon, Fairchild, RCA. Dzięki ich współzawodnictwu powstały: system elektronicznej identyfikacji (1975 r.), elektroniczna tablica rejestracyjna dla pojazdów mechanicznych (1977 r.), biernie kodujący transponder mikrofalowy (1978 r.). W tamtych latach rozwój RFID stymulowało zapotrzebowanie na zdalne tropienie zwierząt i pojazdów oraz automatyzację fabryk. Przykładowo: do znakowania zwierząt wykorzystywano mikrofalowe systemy w Los Alamos oraz indukcyjne systemy w Europie.

Lata osiemdziesiąte stały się dekadą pełnego wprowadzenia technologii RFID w transporcie i kontroli dostępu. Prowadzono także testy RFID przy dokonywaniu elektronicznych opłat, a pierwsze komercyjne zastosowanie miało miejsce w Europie w 1987 roku w Norwegii oraz, w tym samym czasie, w Ameryce – w autobusach jeżdżących przez tunel Lincolna. Pierwsza autostrada z elektronicznym pobieraniem opłat została otwarta w Oklahomie w 1991 roku. Pojazdy mogły przejeżdżać przez punkty pobierania opłat z dużą prędkością, nie będąc zatrzymywanymi przez bramki płatnicze. Pierwszy na świecie system łączący pobór opłat i zarządzanie ruchem drogowym został zainstalowany na obszarze Houston przez Harris County Toll Road Authority w 1992 roku.

Dzisiaj RFID jest technologią, której stosowanie jest powszechne w wielu dziedzinach naszego życia. Dynamiczny rozwój gospodarki światowej generuje duże zapotrzebowanie na systemy automatycznej identyfikacji. Systemy RFID jeszcze przez długie dziesięciolecia będą nam towarzyszyć w logistyce, kontroli dostępu, dokumentach i innych zastosowaniach.

Systemy RFID

Systemy automatycznej identyfikacji radiowej mogą być rozbudowanymi systemami informatycznymi, jak również systemami prostymi, składającymi się z zaledwie kilku elementów. Każdy system RFID, bez względu na stopień złożoności, zawiera następujące elementy:

– identyfikator (tag, transponder, etykieta),
– czytnik,
– oprogramowanie systemowe.

Identyfikator RFID zbudowany jest z układu elektronicznego z pamięcią oraz miniaturowej anteny. Pojemność pamięci identyfikatora wynosi od kilkudziesięciu do kilku tysięcy bitów. Kształt identyfikatora zależy od konkretnego zastosowania. Najczęściej ma on postać prostopadłościanu, krążka czy też karty, wykonanych najczęściej z plastiku. W przypadku kiedy identyfikator ma postać etykiety, układ elektroniczny z anteną zatopiony jest w cienkiej folii.

Wszystkie identyfikatory zawierają układ elektroniczny, który do pracy wymaga dostarczenia odpowiedniej ilości energii. W zależności od sposobu zasilania identyfikatory dzielimy na:

1. Identyfikatory pasywne – wzbudzane przez fale elektromagnetyczne czytnika, nie posiadają własnego źródła zasilania. Odczyt/zapis identyfikatorów pasywnych może odbywać się przy stosunkowo krótkich odległościach (maksymalnie do kilku metrów). Koszt produkcji jest znacznie niższy niż w przypadku identyfikatorów aktywnych.

2. Identyfikatory aktywne – posiadają własne źródło zasilania (baterię) co pozwala na osiągnięcie znacznie większej mocy sygnału transmitowanego z identyfikatora. Ich okres żywotności wynosi – w zależności od trwałości baterii – do pięciu lat. Ich zasięg nadawania wynosi do 100 m, jednakże w porównaniu do identyfikatorów pasywnych są znacznie droższe, a ich zastosowanie jest ograniczone ze względu na mniejszy zakres temperatur pracy oraz większy rozmiar.

Pierwsze identyfikatory nie umożliwiały zmiany zapisanej przez ich producenta informacji. Obecnie niektóre ich typy umożliwiają taką zmianę, co znacznie rozszerza spektrum ich zastosowań. Możemy zatem wyróżnić:

– identyfikatory typu R/O (ang. *Read/Only*) – dane (numer seryjny identyfikatora) są zapisywane w procesie produkcji i nie ma możliwości ich zmiany, jak również zapisu dodatkowych danych,
– identyfikatory typu WORM (ang. *Write Once Read Many Times*) – możliwy jest jednorazowy zapis danych przez użytkownika, bez możliwości zmiany numeru seryjnego,
– identyfikatory typu R/W (ang. *Read/Write*) – można dokonywać wielokrotnego zapisu i odczytu danych, jednak bez możliwości zmiany numeru seryjnego.

Czytnik RFID (dekoder) jest urządzeniem elektronicznym zaopatrzonym w antenę nadawczo-odbiorczą, za pomocą której wysyła lub odbiera wiązkę promieniowania elektromagnetycznego, zapisując lub odczytując w ten sposób dane. Transmisja pomiędzy czytnikiem a identyfikatorem odbywa się w kilku etapach. Najważniejsze z nich to:

1. Etap 1 – czytnik wysyła wiązkę fali radiowej, w identyfikatorze wzbudza się prąd indukcyjny, który zasila układ elektroniczny identyfikatora,
2. Etap 2 – naładowany identyfikator wysyła zwrotnie do czytnika swój unikatowy kod nadany przez producenta lub dane zapisane wcześniej przez użytkownika,
3. Etap 3 – występuje wtedy, gdy chcemy zapisać dane w identyfikatorze.

W rzeczywistości komunikacja przebiega w nieco bardziej złożony sposób. Wykorzystywane są odpowiednie algorytmy kontroli poprawności odczytu/zapisu danych, a także algorytmy weryfikacyjne, zabezpieczające dane przed nieuprawnionym dostępem lub modyfikacją.

Rys. 2. Elementy systemu RFID

Czytniki występują w postaci urządzeń przenośnych, najczęściej zintegrowanych z terminalem i (lub) drukarką etykiet, jak również jako urządzenia stacjonarne, przeznaczone do zabudowy (linie produkcyjne, bramki przy wjeździe do magazynu, bezpośrednio na wózkach widłowych).

Oprogramowanie systemowe odpowiada za fizyczną stronę transmisji (oprogramowanie komunikacyjne) oraz za wymianę, gromadzenie i przetwarzanie danych (oprogramowanie użytkowe). Aplikacje systemu RFID mogą pracować po części na czytniku (w zależności od możliwości samego czytnika), a po części na serwerze – terminalu współpracującym z czytnikiem.

Technologie RFID

Działanie i parametry funkcjonalne urządzeń RFID są mocno uzależnione od zjawisk związanych propagacją fal radiowych. Nie istnieje jedna, idealna do wszystkich zastosowań technologia RFID (częstotliwość). Dlatego też systemy RFID rozwinęły się w trzech pasmach częstotliwości (tab. 1).

Technologia LF powstała jako jedna z pierwszych i jest używana głównie w systemach kontroli dostępu, rejestracji czasu pracy, biletowych, identyfikacji zwierząt itp. Typowy zasięg odczytu/zapisu wynosi około 50 cm. Nie ma możliwości odczytu wielu identyfikatorów jednocześnie. Identyfikatory najczęściej mają postać pastylek, krążków, plastikowych kart. Obecnie nie prowadzi się intensywnych prac nad rozwojem tej technologii.

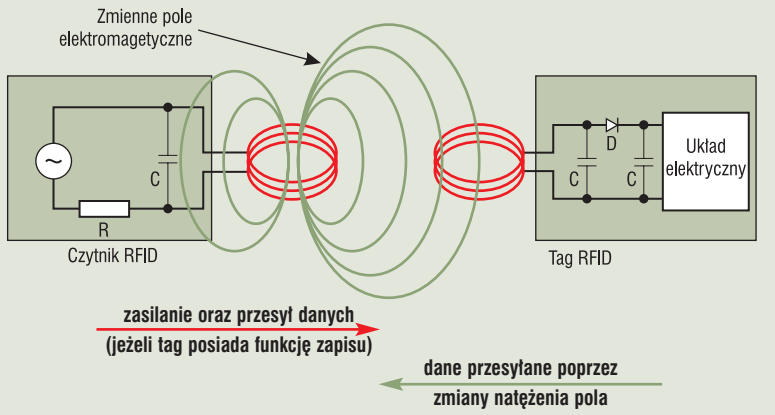
Technologia HF umożliwia odczyt wielu identyfikatorów równocześnie, pod warunkiem, że zachowana jest wymagana minimalna odległość sąsiadujących ze sobą identyfikatorów, wynosząca 2–3 cm. Identyfikatory występują najczęściej w postaci etykiet naklejanych na opakowania. Technologia ta jest wykorzystywana do identyfikacji bagażu na lotnisku, książek w bibliotekach (tylko w kilku bibliotekach na świecie), odzieży w pralniach przemysłowych itp., jednak z powodu małych odległości odczytu, jakie można uzyskać w tym paśmie częstotliwości (maksymalnie 1,5 metra przy dużych antenach), nie znalazła szerszego zastosowania w logistyce.

Technologia RFID w paśmie UHF zapewnia największy zasięg spośród wszystkich częstotliwości dostępnych dla identyfikatorów pasywnych. Jest optymalna do zastosowań w logistyce, przy zarządzaniu łańcuchem dostaw. Z tego też powodu prace nad rozwojem RFID skupiły się szczególnie

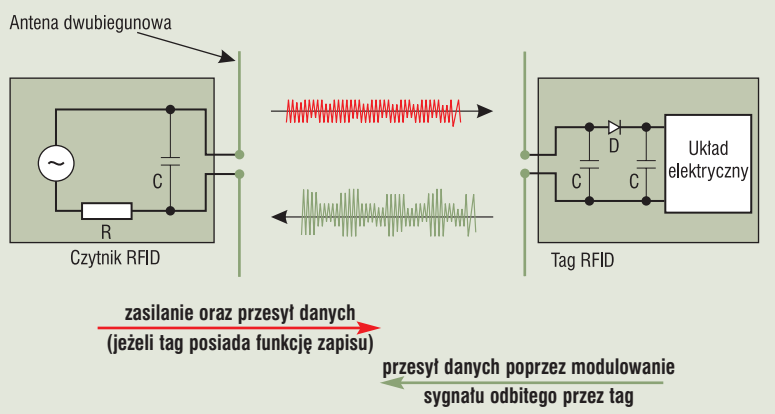
na tym paśmie częstotliwości. Zasięg odczytu wynosi do sześciu metrów w USA. W Europie, z uwagi na mniejsze dopuszczalne moce, zasięg ten jest mniejszy i oscyluje w granicach 2–3 m.

Pasmo mikrofalowe 2,4-5,0 GHz jest wykorzystywane przede wszystkim przez identyfikatory aktywne. Zapewnia duże odległości (ponad 10 m), umożliwiając odczyt danych z obiektów poruszających się z dużą prędkością (powyżej 100 km/h), co jest niemożliwe w technologiach LF i HF. Technologia RFID w paśmie mikrofalowym stosowana jest głównie do identyfikacji i rejestracji obiektów szybko poruszających się (np. w zarządzaniu komunikacją miejską, do rejestracji przejazdu wagonów kolejowych itp.)

Rys. 3. Działanie identyfikatora RFID o częstotliwości pracy poniżej100 MHz



Rys. 4. Działanie identyfikatora RFID o częstotliwości pracy powyżej 100 MHz



Zasada działania

Sposób działania identyfikatorów uzależniony jest od częstotliwości ich pracy. Identyfikatory pasywne, pracujące na częstotliwości do 100 MHz, wykorzystują do zasilania ogólnie znane zjawisko indukcji elektromagnetycznej, powszechnie wykorzystywane w transformatorach energetycznych. Zmienne pole elektromagnetyczne wytworzone w czytniku powoduje indukowanie się siły elektromotorycznej w cewce identyfikatora, która wymusza przepływ prądu elektrycznego. Energia uzyskana w ten sposób jest magazynowana w kondensatorze. Gdy już jest odpowiednia jej ilość, następuje zasilenie układu elektronicznego identyfikatora, który wysyła dane do czytnika poprzez zasilanie cewki (anteny). Można zatem powiedzieć, że komunikacja pomiędzy czytnikiem a identyfikatorem odbywa się dzięki zmianie parametrów pola magnetycznego (rys. 2).

Na maksymalną odległość odczytu/zapisu danych ma wpływ przede wszystkim częstotliwość pracy (wzrost częstotliwości powoduje zmniejszenie zasięgu), a także wymiary geometryczne cewki identyfikatora (im większa cewka, tym większy zasięg). Niestety, względy funkcjonalne nie pozwalają na powiększanie zasięgu przez zwiększanie rozmiaru cewki. Dlatego graniczna odległość dla systemów pracujących na częstotliwości 13,56 MHz wynosi około 30 cm.

Identyfikatory pasywne wyższych częstotliwości (>100 MHz) nie mogą być zasilane z wykorzystaniem zjawiska indukcji magnetycznej, gdyż zasięgi odczytu byłyby niesatysfakcjonujące, dlatego też do zasilenia układu elektronicznego identyfikatora wykorzystuje się w tym przypadku zjawisko przechwytywania energii z odbieranego sygnału, podobnie jak to miało miejsce w dawnych radiach kryształkowych. Przesył danych jest możliwy dzięki wykorzystaniu zjawiska rozproszenia wstecznego fali radiowej. Identyfikator, poprzez zmianę (według określonego wzorca) parametrów impedancyjnych anteny, odbija część fali z powrotem w kierunku czytnika. W ten sposób następuje wymiana danych (rys. 3). Odległości graniczne, jakie uzyskano w systemach wykorzystujących powyższe zjawiska fizyczne, oscylują w granicach 10 m.

Tab. 1. Pasma pracy systemów RFID

Częstotliwość	Zastosowania
LF (10-500 kHz)	Rejestracja dokumentów, przedmiotów niemetalowych, przedmiotów płynnych ludzi i zwierząt – **mała przepustowość**
HF (10-15 MHz)	Rejestracja dokumentów, przedmiotów niemetalowych, przedmiotów płynnych ludzi i zwierząt – **duża przepustowość**
UHF (860-960 MHz) Mikrofale (2,4-5,0 GHz)	Śledzenie kontenerów, palet, pojazdów, materiałów metalowych – **duża przepustowość**

W zależności od producenta stosowane są różne częstotliwości, sposoby modulacji sygnału oraz rodzaje fal. Do trzech podstawowych technik modulacji stosowanych w systemach RFID należą:

- modulacja amplitudy AM (ang. *Amplitude Modulation*) – stosowana w identyfikatorach pasywnych działających na częstotliwości poniżej 100 MHz,
- modulacja fazy PM (ang. *Phase Modulation*) – stosowana w identyfikatorach pasywnych działających na częstotliwości powyżej 100MHz,
- modulacja częstotliwości FM (ang. *Frequency Modulation*).

Przedstawione w artykule ogólne wiadomości z zakresu historii i zasad działania RFID stanowią zaledwie wstęp do bardziej szczegółowych rozważań dotyczących zastosowań, a przede wszystkim zagrożeń, z jakimi możemy mieć do czynienia, używając technologii radiowej identyfikacji.

Przemysław Mierzwiak
Instytut Inżynierii Systemów Bezpieczeństwa

Literatura:

1. Klaus Finkenzeller: *RFID Handbook*, John Wiley & Sons Ltd., 2003.
2. AIM Inc.: *The History of RFID*, 2001.
3. Michał Grabia: *Zasada działania technologii RFID*, *http://www.e-fakty.pl,* 5/2006.
4. *http://www.skk.com.pl.*

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

HDP5000 – nowa drukarka FARGO

Czy jakość wydruku retransferowego na karcie plastikowej jest warta ceny, jaką trzeba zapłacić za odpowiednią do tego celu drukarkę?

Wiele firm i instytucji odpowiedziało sobie twierdząco na powyższe pytanie już wiele lat temu i do dziś korzysta z zadowoleniem ze starszych modeli drukarek Fargo serii HDP. Dla niezdecydowanych głównym argumentem przeciwko wyborowi drukarek retransferowych była ich cena. Aż do dziś…

Amerykańska firma Fargo Electronics, renomowany producent drukarek do kart plastikowych, wykonała kolejny krok w kierunku upowszechnienia technologii druku retransferowego. Wprowadzając na rynek drukarkę HDP5000, Fargo ustaliło ceny tego modelu na wyjątkowo atrakcyjnym poziomie, co pozwoliło na skierowanie oferty drukarek High Definition (najwyższa jakość nadruku) do segmentu klientów zainteresowanych dotychczas wyłącznie tańszymi modelami takich urządzeń.

Co to oznacza dla potencjalnych odbiorców? Oznacza to, że wydruk identyfikatorów lub kart klienta w jakości High Definition jest teraz dostępny dla dużo szerszego grona odbiorców.

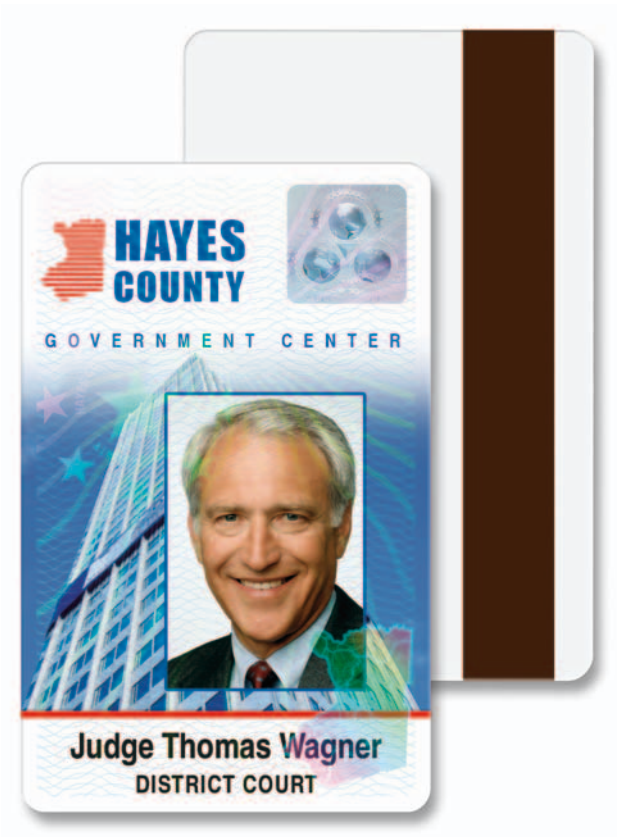
Atrakcyjna cena drukarki nie wpłynęła ujemnie na jakość urządzenia, co więcej – w HDP5000 wprowadzono szereg ulepszeń w stosunku do poprzedniego modelu – HDP600. Modułowa budowa umożliwia klientom skonfigurowanie drukarki zgodnie z ich wymaganiami. To klienci decydują, czy potrzebują drukarkę do wydruku jedno- czy dwustronnego, z laminacją czy bez oraz z jakimi koderami. Co więcej, poszczególne moduły można dodawać później, w trakcie eksploatacji drukarki, kiedy zaistnieje konieczność jej rozbudowy.

Innym ciekawym rozwiązaniem jest możliwość jednoczesnej laminacji obu stron karty: w module laminacyjnym instalowane są dwie taśmy i laminowane są obie strony karty przechodzącej przez ten moduł w tym samym czasie – znacznie zwiększa to wydajność drukarki, skracając czas zadruku karty.

Kolejną innowacją jest standardowe wyposażenie HDP5000 w dwa wejścia: USB oraz Ethernet (z wewnętrznym serwerem wydruku). Umożliwia to użytkownikom instalację drukarki do pracy jednostanowiskowej bądź w sieci komputerowej, w zależności od potrzeb. Z portami drukarki wiąże się jeszcze jedna istotna zaleta tego modelu: kodery instalowane w tym urządzeniu obsługiwane są przez wymienione wyżej wejścia; nie ma potrzeby, a nawet możliwości, podłączania ich oddzielnie. Ta technologia, nazwana przez producenta ‘One Wire’, jest nowatorskim i jedynym takim rozwiązaniem na rynku drukarek do kart.

Następnym udogodnieniem dla użytkowników jest umieszczenie taśm do nadruku w kasetach, co znacznie ułatwia i przyspiesza ich instalację w drukarce. To rozwiązanie jest już stosowane w prostszych drukarkach Fargo, np. Persona C30 czy DTC400, i spotkało się z bardzo pozytywnym przyjęciem przez użytkowników.

Poza wymienionymi wyżej udoskonaleniami, HDP5000 posiada wszystkie cechy, które dotychczas sprawiały, że drukarki Fargo serii High Definition cieszyły się tak wysokim uznaniem użytkowników. Podstawową zaletą jest retransferowa technologia nadruku, polegająca na nanoszeniu obrazu na specjalną warstwę folii HDP (*High Definition Printing*), a następnie nanoszeniu jej przez laminację na kartę. Takie rozwiązanie pozwala osiągnąć bardzo wysoką jakość nadruku, zbliżoną do druku offsetowego, i zadruk całej powierzchni karty, od krawędzi do krawędzi, wraz z ewentualnymi nierównościami na karcie.



Drukarki Fargo HDP świetnie sprawdziły się przy personalizacji Elektronicznych Legitymacji Studenckich. Są użytkowane przez ponad 30 polskich uczelni wyższych. Model HDP5000 spotkał się z dużym zainteresowaniem uczelnianych centrów personalizacji. Pierwsze egzemplarze tego modelu już pracują przy wydruku i personalizacji nowych legitymacji.

Więcej informacji o drukarkach Fargo można uzyskać na www.cs.pl lub bezpośrednio u wyłącznego dystrybutora Fargo w Polsce, w firmie Control System FMN, tel.: (22) 855-00-17.

Paweł Kornacki
Control System FMN

urmet
MIWI

iProtect™

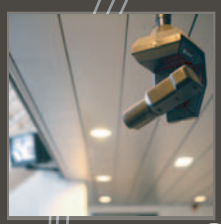
ZINTEGROWANY SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM

TCP/IP

Kontrola Dostępu

Rejestracja Czasu Pracy

TCP/IP



CCTV IP

TCP/IP

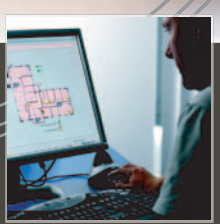
SSWiN

TCP/IP

Rejestracja Gości

TCP/IP

Parking



Integracja z systemem PPOŻ

Ochrona Osób

MIWI-URMET sp. z o.o., 91-341 Łódź, ul. Pojezierska 90A, www.miwiurmet.com.pl, e-mail:miwi@miwiurmet.com.pl

iProtect – sieciowy system zabezpieczenia obiektów

Zintegrowany system zarządzania bezpieczeństwem *iProtect* holenderskiej firmy Keyprocessor oferuje bogatą funkcjonalność w zakresie zabezpieczeń elektronicznych. Jest to system modułowy, w którym różne funkcje mogą być dodawane zgodnie z potrzebami klienta. Rozbudowa systemu, zarówno sprzętowa jak i funkcjonalna, może odbywać się później, już podczas jego użytkowania.

Krótki opis systemu *iProtect*

System ***iProtect*** bazuje na najnowszych technologiach teleinformatycznych, a do komunikacji wykorzystuje sieć TCP/IP. Struktura systemu pozwala na instalowanie go z wykorzystaniem sieci strukturalnej. Okablowanie jest uproszczone (skrętka UTP kat. 5), dzięki czemu koszty instalacji, rozbudowy i konserwacji systemu są niskie.

iProtect to kompletne rozwiązanie służące do zarządzania bezpieczeństwem obiektów i organizacji średniej i dużej wielkości, integrujące wiele systemów zabezpieczeń elektronicznych.

Na zintegrowany system zarządzania bezpieczeństwem *iProtect* składa się:
– kontrola dostępu (KD) dla nieograniczonej liczby czytników i 100000 użytkowników,
– system sygnalizacji włamania i napadu (SSWiN),
– system telewizji dozorowej (współpraca z rejestratorami IP Milestone lub kamerami IP) z weryfikacją wideo,
– rejestracja czasu pracy (RCP) – standardowo dla 3000 pracowników, z możliwością rozszerzenia;
– zarządzanie parkingiem (także parkingiem płatnym, rozbudowanym, dla wielu firm oraz gości),
– ochrona osób.

Możliwe jest współdziałanie z systemem sygnalizacji pożaru, z którego sygnały mogą być doprowadzone do wejść kontrolerów *iProtect* i wywoływać określone reakcje w systemie (np. odblokowywać drzwi ewakuacyjne). Jedna z aplikacji służy do opracowywanie projektów nadruku na kartach (Photo-ID). System umożliwia także rejestrację gości.

Cechy charakterystyczne systemu to między innymi:
– wykorzystanie sieci TCP/IP,

– wizualizacja za pomocą interaktywnych map,
– niezależne od lokalizacji zarządzanie systemem,
– pełna skalowalność.

Cechą charakterystyczną systemu *iProtect* jest także wykorzystywanie otwartych standardów (TCP/IP, JDBC, ODBC, JSP, XML). Dotyczy to zarówno oprogramowania, jak i identyfikacji za pomocą technologii *smart card.* Dzięki otwartym standardom integracja systemu iProtect z systemami innych producentów (np. systemami kadrowo płacowymi, BMS, wielofunkcyjnymi aplikacjami *smart card*) jest łatwa w realizacji.Aplikacje systemu uruchamiane są poprzez sieć TCP/IP, a komunikacja między serwerem *iProtect* a stacjami roboczymi jest szyfrowana za pośrednictwem protokołu SSL. Dzięki temu nie jest wymagana instalacja dedykowanego oprogramowania na komputerach klienckich. Zarządzanie systemem, w tym także wejściami i wyjściami, jest możliwe z dowolnej lokalizacji – potrzeba tylko połączenia sieciowego z serwerem oraz przeglądarki Internet Explorer (*iProtect* jest kompatybilny z przeglądarką Internet Explorer – wersją 6.0 SP1 oraz 7.).

Elastyczność i skalowalność systemu

System iProtect został zaprojektowany z myślą o optymalnej elastyczności. Każdy moduł programowy jest niezależny i może pracować autonomicznie. Kolejne moduły mogą być bezproblemowo dodawane do istniejącej instalacji *iProtect*.

Jednak *iProtect* jest elastyczny nie tylko w zakresie oprogramowania, ale również w zakresie sprzętu. Kolejne czytniki, kamery, czujki alarmowe czy terminale RCP mogą być dodawane zgodnie z bieżącymi potrzebami.

iProtect jest więc systemem całkowicie skalowalnym. Inwestycja może rozpocząć się od małego systemu, a z biegiem czasu i w miarę wzrostu potrzeb można go powiększać i sprawić, by stał się bardziej wielofunkcyjny. Nie koliduje to z wcześniejszą inwestycją. Dzięki najnowszej technologii sieciowej jeden system może połączyć obiekty oddalone od siebie, zlokalizowane w różnych miejscach (np. oddziały firm).

Urządzenia

iProtect wykorzystuje niezawodne, specjalizowane jedno- lub dwuprocesorowe serwery firmy Sun Microsystems ze specjalnie przygotowanym systemem operacyjnym Solaris Unix (średni czas do wystąpienia uszkodzenia MTBF – ang.: *Mean Time Before Failures* – to ponad 4.6 lat) oraz kontrolery Orbit i technologię jednostek sieciowych Stellar.

Kontrolery współpracują z czytnikami cyfrowymi, działającymi na częstotliwości 125 kHz lub 13.56 Mhz). Jedna karta dostępu jest wykorzystywana w wielu aplikacjach. Obrazy linii papilarnych zapisywane są na karcie użytkownika, bez archiwizacji na serwerze, co znacznie podnosi bezpieczeństwo systemu oraz szybkość jego działania.

Technologie obniżające koszty

W systemie *iProtect* komunikacja pomiędzy kontrolerami sieciowymi Stellar a serwerem oraz między komputerami klienckimi a serwerem odbywa się za pośrednictwem sieci TCP/IP. Oznacza to, że *iProtect* może być z łatwością stosowany w istniejących sieciach LAN i WAN. Jak wcześniej wspomniano aplikacja *iProtect* uruchamiana jest poprzez sieć na komputerach klienckich z wykorzystaniem przeglądarki Internet Explorer dzięki czemu:
– komputer z przeglądarką Internet Explorer i podłączeniem do sieci jest wszystkim, czego potrzebuje operator systemu,
– nie jest wymagane instalowanie specjalnego oprogramowania na komputerach klienckich,
– korzystanie z aplikacji *iProtect* nie jest związane z konkretnym miejscem czy komputerem,
– problemy związane z różnymi wersjami systemów operacyjnych należą do przeszłości.

Intuicyjność i łatwość obsługi

Oprogramowanie *iProtect* jest nie tylko przyjemne dla oka, ale także, co ważniejsze, łatwe w użyciu i wysoce intuicyjne. Wszystkie ekrany mają ten sam czytelny układ. Przedstawianie wielu danych w formie struktury drzewa powoduje, że informacje są łatwo dostępne, a zależność elementów jest bardzo przejrzysta.

Unikatowy generator raportów

Dobre raportowanie ma kluczowe znaczenie w przypadku dużych systemów bezpieczeństwa i RCP. Właśnie z tego powodu w systemie *iProtect* znajduje się rozbudowany generator raportów. Przygotowanie odpowiedniego raportu jest łatwe. Dane przedstawiane są w przejrzystej formie. Dzięki zastosowaniu między innymi formatu PDF raporty mogą być z łatwością drukowane, zapisywane, przesyłane pocztą elektroniczną i archiwizowane.

Powyżej przedstawiono jedynie podstawowe informacje o systemie iProtect. Bardziej szczegółowe, zarówno dotyczące oprogramowania, jak i urządzeń, znajdą się na naszych łamach w kolejnych artykułach na temat poszczególnych aplikacji tego systemu.

Łukasz Szafoni
Miwi-Urmet

PROTECTOR

System Kontroli Dostępu
i
Rozliczania Czasu Pracy
z
ELEMENTAMI AUTOMATYKI
„SOYAL"

- Darmowy program obsługi systemu KD oraz RCP
- Pojemność systemu -15 tysięcy użytkowników
- Praca kontrolerów samodzielna lub w sieci
- Możliwość kontroli 4064 drzwi
- Zakres temperatur pracy kontrolerów do -10°C, czytników do -20 °C
- Współpraca z wieloma czytnikami w różnych formatach (WG26/34, ABA, 125KHz, 13,56 MHz Mifare, 2,4 GHz)
- Pełna integracja z systemami CCTV oraz SSWiN

Kontroler z wew. czytnikiem oraz wyświetlaczem LCD wodoszczelny już od:

599zł netto

Czytnik z klawiaturą już od:

209zł netto

Czytnik już od:

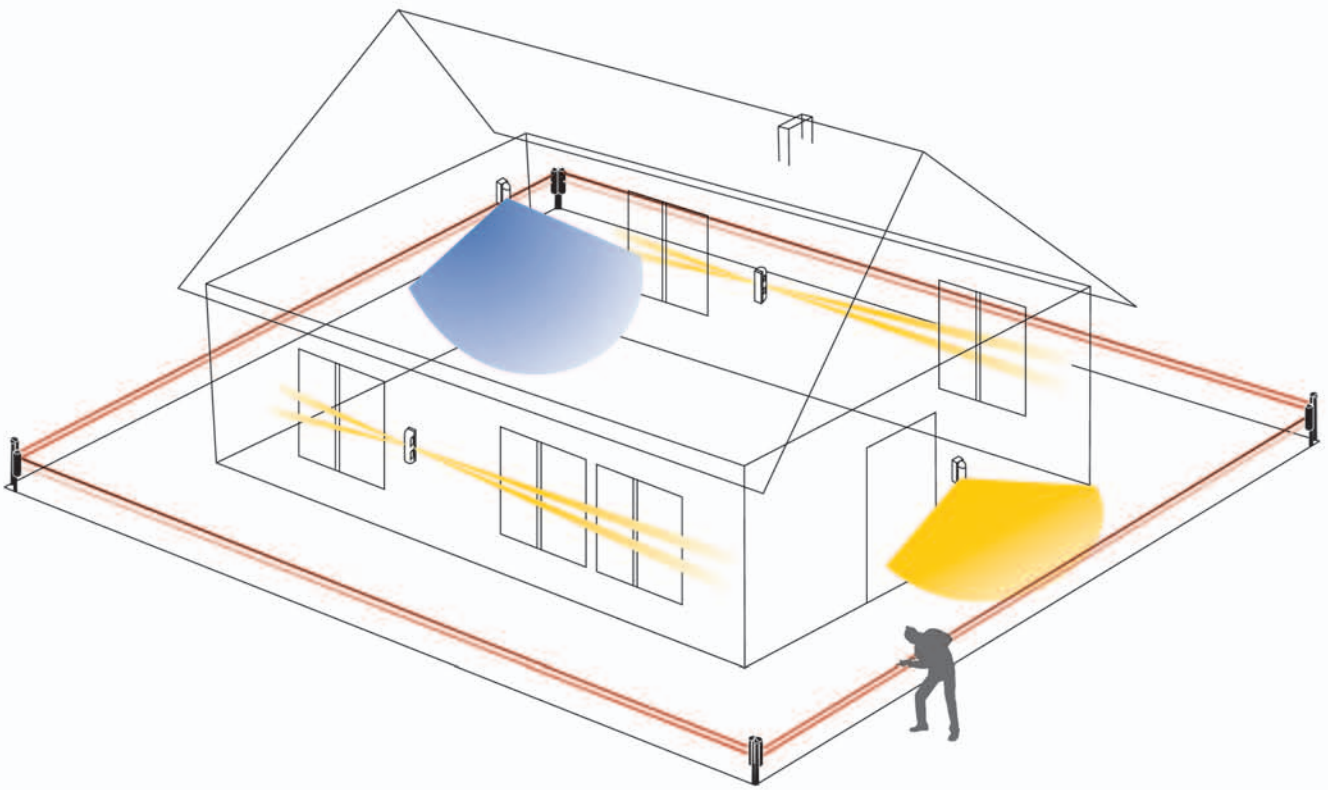
159zł netto

www.protector-polska.pl

tel: +48 (091) 431 83 10
fax: +48 (091) 431 83 11

biuro@protector-polska.pl

TRÓJSTREFOWA ochrona



Firma Optex stworzyła niezawodny, kompleksowy system urządzeń, wykrywających wtargnięcie intruza na teren obiektu chronionego, jak i na jego obrzeża. System składa się z trzech stref ochrony obiektu:

• STREFA OCHRONY WEWNĘTRZNEJ

Chroni pomieszczenia obiektu.

W tej strefie zastosowanie znajdują pasywne czujki podczerwieni, czujki dualne (PIR + mikrofala) oraz bariery podczerwieni.

- RX-40QZ/40PT
- MX-40QZ/50QZ
- CX-502AM
- CX-702
- FX-360
- SX-360Z
- AX-100S/100SR

• STREFA OCHRONY ZEWNĘTRZNEJ

Chroni elewację budynku oraz obszar pomiędzy ogrodzeniem a obiektem.

W tej strefie zastosowanie znajdują pasywne czujki podczerwieni oraz bariery podczerwieni.

- LX-402
- LX-802N
- VX-402/402REC
- BX-80N
- BX-100PLUS

• STREFA OCHRONY OBWODOWEJ

Chroni obwód terenu wokół budynku.

W tej strefie zastosowanie znajdują cyfrowe i analogowe bariery podczerwieni krótkiego i dalekiego zasięgu.

- AX-70TN/130TN/200TN
- AX-100TF/200TF
- AX-250PLUS/500PLUS
- AX-350TF/650TF
- AX-350/650DH MK III

Te trzy poziomy bezpieczeństwa zapewniają pewną ochronę obiektu i polepszają działania prewencyjne.

Specyfikacja techniczna

OCHRONA WEWNĘTRZNA

	RX-40QZ/40PT	MX-40QZ	MX-50QZ	CX-502AM	CX-702	FX-360	SX-360Z	AX-100S/100SR
								
W domach	✓	✓	✓	–	–	✓	–	✓
W małych biurach	✓	✓	✓	–	–	✓	✓	✓
W dużych biurach	–	–	✓	✓	✓	–	✓	–
W pomieszczeniach przemysłowych	–	–	–	✓	✓	–	–	–
Zasięg detekcji	12x12m	12x12m	15x15m	15x 5m	21x21m 45x2,4m	Ø18-20m	Ø18m	30m
Zasilanie	9,5 - 16V=	9,5 - 16V=	9,5 - 16V=	9 - 18V=	9,5 - 16V=	9,5 - 18V=	6 - 18V=	8 - 18V=
Pobór prądu (odbiornik + nadajnik)	17mA maks.	18mA maks.	20mA maks.	19mA maks.	11mA	18mA maks.	18mA maks.	52mA maks. odbiornik+nadajnik
Temperatura pracy	-20°C - +50°C	-10°C - +55°C	-10°C - +55°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C

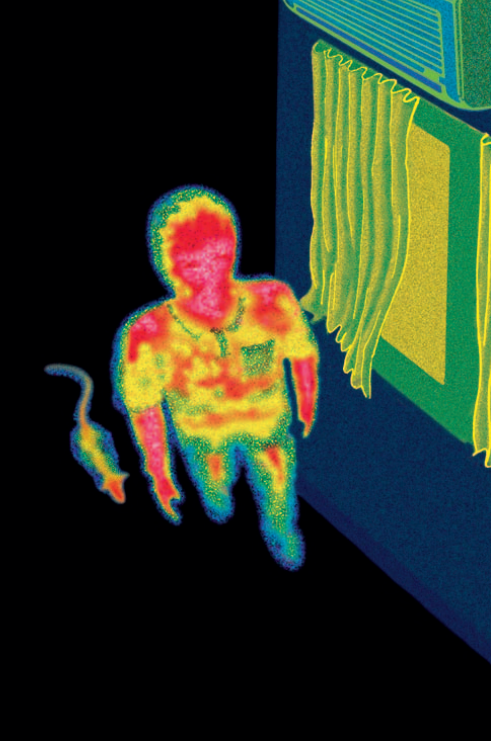
OCHRONA ZEWNĘTRZNA

	LX-402	LX-802N	VX-402	VX-402REC	BX-80N	BX-100PLUS
						
W domach	✓	✓	✓	✓	✓	✓
W małych biurach	✓	✓	✓	✓	✓	✓
W dużych biurach	–	✓	✓	✓	✓	–
W pomieszczeniach przemysłowych	–	–	✓	✓	✓	–
Współpraca z CCTV	✓	✓	✓	✓	✓	–
Zasięg detekcji	12 x 15m	24 x 2m	12m 90°	12m 90°	24m (12m na każdą stronę)	30m
Zasilanie	10,8 - 13.2V =	10,8 - 13,2V =	9,5 - 18V =	9,5 - 18V =	10 - 28V =	10,5 -30V =
Pobór prądu	25mA maks.	25mA maks.	NC : 28mA maks. NO : 35mA maks.	NC : 180mA maks. NO : 200mA maks.	38mA maks.	75mA maks.
Klasa ochrony IP	IP54	IP54	IP54	IP54	IP55	IP54
Temperatura pracy	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-35°C - +55°C

OCHRONA OBWODOWA

	AX-70TN/AX-130TN	AX-200TN	AX-100TF/AX-200TF	AX-250PLUS/AX-500PLUS	AX-350TF/AX-650TF	AX-350DH MKIII/AX-650DH
						
W domach	✓	✓	–	–	–	–
W małych biurach	✓	✓	✓	–	–	–
W dużych biurach	–	–	✓	✓	✓	✓
W pomieszczeniach przemysłowych	–	–	✓	✓	✓	✓
Zasięg detekcji	20m/40m	60m	30m/60m	75m/150m	100m/200m	100m/200m
Zasilanie	10,5 - 28V =	10,5 - 28V =	10,5 - 28V =	10,5 - 30V =	10,5 - 30V =	10,5 - 30V =
Pobór prądu (odbiornik + nadajnik)	38mA maks./41mA maks.	45mA maks.	44mA maks./48mA maks.	50mA maks.	78mA maks./80mA maks.	105mA maks./110mA maks.
Klasa ochrony IP	IP65	IP65	IP65	IP54	IP54	IP65
Temperatura pracy	-35°C - +60°C	-35°C - +60°C	-35°C - +60°C	-25°C - +55°C	-35°C - +60°C	-35°C - +60°C

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; e-mail: aat.warszawa@aat.pl



Technologie detekcji

firmy Optex

W tym roku na łamach *Zabezpieczeń* ukazało się kilka artykułów o produktach firmy Optex, przodującego producenta urządzeń służących do ochrony obiektów. Wiele miejsca poświęcono w nich funkcjonalności produktów. Niniejszy artykuł, podsumowujący cykl, skupia się na kilku najważniejszych technologiach, które zapewniają długotrwałą i niezawodną pracę czujek.

Firma Optex specjalizuje się w rozwijaniu technologii optycznych, co daje jej produktom przewagę nad konkurencją. Aby wykorzystać zjawisko emisji promieniowania podczerwonego w czujkach PCP, należy przede wszystkim starannie zaprojektować i precyzyjnie wykonać układy optyczne. To one są odpowiedzialne za odpowiednie wychwytywanie promieniowania podczerwonego z otoczenia, które jest później przetwarzane na impulsy elektryczne i analizowane w układach elektronicznych.

Technologia *Multi-Focus Optics*

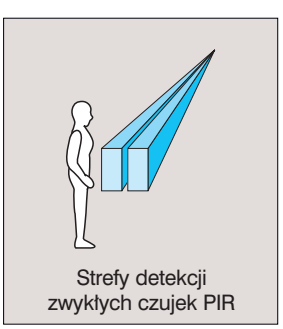
Z zastosowaniem technologii PCP w czujkach ruchu wiążą się pewne trudności, które wynikają z natury promieniowania podczerwonego, posiadającego własności fizyczne zbliżone do światła widzialnego. Wyposażenie biur lub magazynów w biurka, regały i inne sprzęty powoduje, że zamontowane w takich pomieszczeniach czujki ruchu mają ograniczone pole widzenia. Przesłonięcie stref czułości elementami wyposażenia powoduje ograniczenie pola detekcji i powstawanie tzw. martwych stref, w których wykrycie intruza staje się niemożliwe. **Technologia *Multi-Focus Optics*** powstała jako odpowiedź na zapotrzebowanie rynku na czujki, dzięki którym ryzyko występowania martwych stref jest mniejsze. Istotą tej technologii jest zmiana proporcji stref czułości oraz zwiększenie ich liczby w pionie. W stosunku do detektorów konkurencji czujki firmy Optex wyposażone w tę technologię dysponują nawet dwukrotnie większą gęstością pionową stref czułości. Zmiana proporcji samej strefy czułości, polegająca na jej wydłużeniu, zaowocowała większą powierzchnią pokrycia źródła promieniowania podczerwonego.

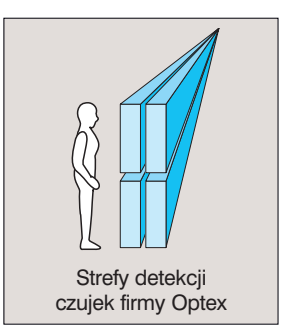
Technologia *Quad-Zone Logic*

Zwiększanie czułości dostępnych na rynku detektorów za wszelką cenę spowodowało destabilizację ich pracy i generowanie dużej liczby fałszywych alarmów. To zjawisko jest zmorą instalatorów systemów zabezpieczeń z dwóch powodów. Pierwszym są rosnące koszty obsługi obiektu ze względu na częste wezwania patroli interwencyjnych, drugim – niezmiernie istotnym – malejąca czujność i uwaga, jaką poświęcamy sygnałowi alarmowemu. Na niektórych rynkach doprowadziło to niemalże do wyeliminowania sygnalizatorów z instalacji alarmowych (np. w Czechach). Poszukując rozwiązania tego problemu, inżynierowie firmy Optex znaleźli sposób na to, aby wprowadzić do analizy jeszcze jeden parametr – rozmiary źródła promieniowania. W ten sposób ewolucja **technologii *Multi-Focus Optics*** doprowadziła do powstania **technologii *Quad-Zone Logic***, która minimalizuje wpływ niewielkich, w stosunku do rozmiarów człowieka, źródeł promieniowania podczerwonego na pracę czujki alarmowej. Podobnie jak w przypadku jej poprzedniczki, również i tym razem system optyczny gra zasadniczą rolę. Zwielokrotnienie stref detekcji powoduje, że obiekty większe są pokryte większą liczbą stref czułości niż obiekty mniejsze. Wynikiem tego jest istotne uzależnienie poziomu promieniowania docierającego do przetwornika od rozmiarów obiektu. I tak, obiekt rozmiarów człowieka – w zamyśle powodujący aktywację alarmu – będzie pokryty strefami czułości w liczbie od czterech do ośmiu, powodując kilkukrotnie większe skupienie promieniowania na elemencie przetwornika niż w przypadku obiektów relatywnie niewielkich rozmiarów (np. małych zwierząt), pokrytych jedną strefą czułości. Ta niezwykła technologia, nazywana często „quadem logicznym", przez analogię do czujników używających poczwórnych pyroelementów do zwielokrotnienia sygnału po stronie elektrycznej, jest w istocie

Technologie *Quad-Zone Logic* i *Multi-Focus Optics*

Zwykle w czujnikach PIR wykorzystywany jest podwójny pyroelement, który formuje dwie strefy detekcji. Czujki firmy Optex maja znacznie wiecej pionowych stref detekcji.
Zastosowanie wyzszych stref detekcji pozwala na lepsze odróznienie człowieka od innych zródeł podczerwieni, a także na wykrycie małych zmian temperatury, gwarantujac niezawodna detekcje.


Strefy detekcji zwykłych czujek PIR


Strefy detekcji czujek firmy Optex

„quadem optycznym", który dokonuje zwielokrotnienia sygnału docierającego do przetwornika po stronie optycznej. Silna zależność od rozmiarów źródła promieniowania umożliwiła stworzenie detektorów, których prawidłowego funkcjonowania nie mogą zakłócić zwierzęta domowe.

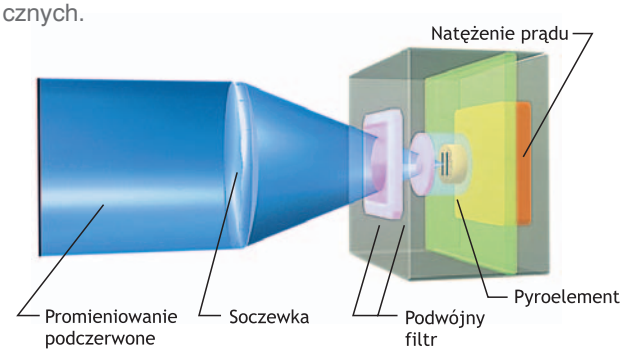
Technologia *Double Conductive Shielding*

Czujki PCP są często wystawione na oddziaływanie zakłóceń elektromagnetycznych powodowanych przez urządzenia biurowe, maszyny elektryczne itp., dlatego podczas projektowania czujek należy zwrócić szczególną uwagę na ich odporność na tego typu zakłócenia. Mimo że dosyć łatwo, stosując ogólnie znane metody projektowania, zabezpieczyć układy elektroniczne, nie jest to proste w przypadku samego elementu przetwornika. Pyroelement jest wykonany z materiału światłoczułego, przetwarzającego promieniowanie podczerwone na impulsy elektryczne. Jest niezmiernie czuły na wszelkiego rodzaju pobudzenia elektromagnetyczne. Zasada działania czujki wyklucza pełne ekranowanie tego elementu ze względu na dostęp do przetwornika promieniowania podczerwonego z otoczenia. Chociaż sam w sobie posiada on własności selektywne, nie jest w pełni odporny na pobudzenia światłem o innych długościach fali (np. światłem widzialnym). Aby zminimalizować wpływ tego typu pobudzeń na pracę czujek, każdą dostępną na rynku czujkę ruchu PCP wyposaża się w filtr światła białego. Najczęściej jest to nieprzezroczysty dodatek w materiale soczewki oraz warstwa półprzewodnika na obudowie pyroelementu. W wielu przypadkach nie zapewnia to wystarczającej ochrony i wówczas możemy zaobserwować fałszywe alarmy spowodowane np. przez oświetlenie czujnika silnym strumieniem światła lamp halogenowych lub odbiciami światła słonecznego. Szczególnym utrudnieniem jest fakt, iż w przyrodzie występuje niewiele materiałów przepuszczających promieniowanie podczerwone, takich jak polietylen czy niektóre półprzewodniki.

Double Conductive Shielding to kolejna flagowa technologia firmy Optex, która powstała z połączenia tych dwóch materiałów. Cienka warstwa półprzewodnika naniesiona na elastyczną polietylenową płytkę tworzy zaporę dla światła widzialnego, przepuszczając wyłącznie promieniowanie podczerwone. Skuteczność filtru w stosunku do światła białego określa się na 50000 lx. Zdolność przewodzenia ładunków elektrycznych umożliwiła pełne ekranowanie pyroelementu i uzyskanie urządzeń o wyjątkowej odporności na zakłócenia elektromagnetyczne. Stosowanie filtrów ***Double Condctive Shielding*** umożliwia niezawodną pracę czujek przy zakłóceniach elektromagnetycznych sięgających 30 V/m w szerokim zakresie częstotliwości.

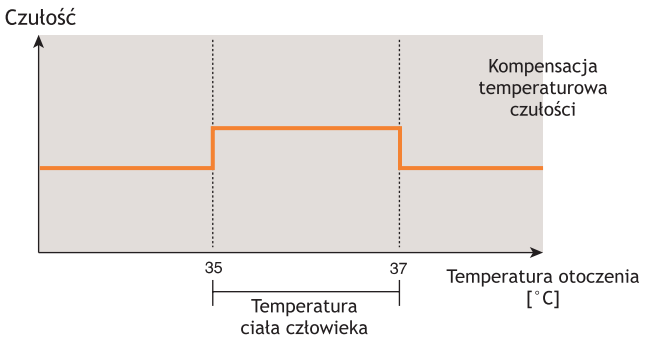
Technologia *Double Conductive Shielding*

Czujki, w których zastosowano opatentowana technologię *Double Conductive Shielding* posiadaja właściwosci ltracji fal z zakresu swiatła widzialnego, jak i fal elektromagnetycznych.



Technologia *Advanced Temperature Compensation*

Technologia *Advanced Temperature Compensation* reguluje poziom wzmocnienia sygnału w zależności od temperatury otoczenia, zmieniając intensywność tej regulacji w zakresie temperatur od 35 do 37 stopni Celsjusza.



Technologia *Advanced Temperature Compensation*

Innym problemem dotyczącym warunków pracy czujek PCP jest niski kontrast pomiędzy promieniowaniem tła i promieniowaniem emitowanym przez człowieka w temperaturze zbliżonej do temperatury ciała człowieka. W takich warunkach zaobserwowanie zmian promieniowania jest niezwykle trudne i niemalże wyklucza prawidłową detekcję ruchu. Już wczesne konstrukcje próbowano wyposażyć w mechanizmy dostosowujące parametry pracy czujek do warunków otoczenia. Najprostszym rozwiązaniem jest oczywiście pętla automatycznej regulacji wzmocnienia, zależna od poziomu promieniowania tła lub temperatury otoczenia. Ma ona jednak swoje istotne ograniczenia, np. wzmocnieniu podlega zarówno sygnał użyteczny, jak i szumy pochodzące z promieniowania tła oraz zakłóceń termicznych układów elektronicznych. Jeszcze bardziej istotne jest występowanie zjawiska inwersji, tzn. po przekroczeniu temperatury 39°C kontrast pomiędzy promieniowaniem tła a człowieka zaczyna się ponownie zwiększać. Dalsze zwiększanie wzmocnienia powoduje destabilizację pracy czujki i w konsekwencji zwiększenie liczby fałszywych alarmów. Dlatego producenci czujek PCP używanych w systemach alarmowych stosują różne metody rozwiązywania tego problemu. Firma Optex zastosowała w swoich detektorach **technologię** *Advanced Temperature Compensation*, która reguluje poziom wzmocnienia sygnału w zależności od temperatury otoczenia, zmieniając intensywność tej regulacji w zakresie temperatur od 35 do 37 stopni Celsjusza. Dzięki temu układ realizujący algorytm identyfikacji intruza otrzymuje na wejściu sygnał o stabilnych parametrach, niezależnie od temperatury otoczenia, co w znaczący sposób wpływa na poprawność wykrywania intruza.

To jedynie kilka z bardzo wielu technologii firmy Optex, stosowanych w produktach oferowanych klientom na całym świecie. Stanowią one dowód na to, jak wielką wagę przykłada firma do rozwoju technologicznego produktów. Celem firmy Optex jest dostarczanie rozwiązań na miarę potrzeb klientów. Potrzeby te są zawsze w centrum zainteresowania firmy i pracowników działów badań i rozwoju.

Wszystkie produkty Optex są do nabycia w firmie *AAT-T,* która jest autoryzowanym dystrybutorem firmy Optex w Polsce.

Jarosław Gibas
Optex Security

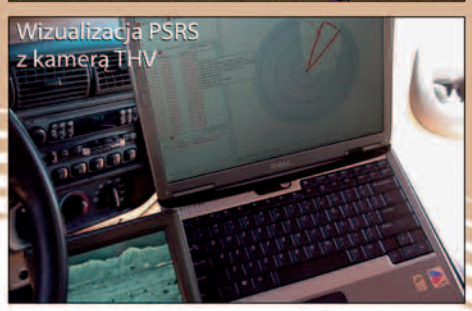
KABE

Najnowsza
technologia ochrony
rozległych terenów zewnętrznych

RADARY

Idealne zabezpieczenie
dla lotnisk i baz wojskowych


Radar RDTS
na granicy USA


Wizualizacja PSRS
z kamerą THV


Radar PSRS
z kamerą THV

Systemy radarowe wykrywają każde
wtargnięcie na chroniony obszar i stale
monitorując aktualną pozycję intruza
mogą sterować zintegrowanym
systemem nadzoru wizyjnego

KABE

43-190 MIKOŁÓW
ul. Waryńskiego 63

www.kabe.pl
e-mail: handel@kabe.pl

tel.: (+48 32) 32 48 900
faks: (+48 32) 32 48 901

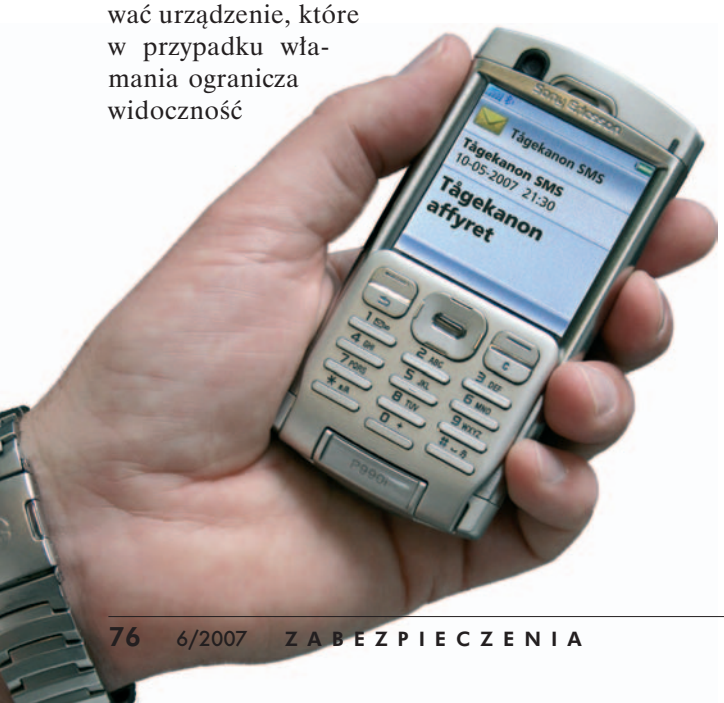
artykuł sponsorowany

Działko dymne Fog Cannon SMS firmy Protect

Od początku 2007 roku firma AWC Protect Global System Polska zajmuje się wyłączną dystrybucją urządzeń zamgławiających duńskiej firmy Protect, która od wielu lat jest wiodącym światowym dostawcą dymnych zabezpieczeń obiektów. Obecnie na terenie Polski współdziałamy z kilkunastoma firmami branży zabezpieczeń technicznych i fizycznej ochrony mienia. Wizją firmy jest skuteczna ochrona wszystkiego, co stanowi wartość dla klientów

Urządzenia zabezpieczające Protect są konstruowane w sposób, który pozwala zintegrować je z tradycyjnymi systemami antywłamaniowymi. Kiedy włamywacz aktywuje alarm, pomieszczenie wypełnia się gęstym, lecz nieszkodliwym dymem. Zabezpieczenie to skutecznie zatrzymuje włamywacza w czasie krótszym niż 20 sekund. Konwencjonalne systemy antywłamaniowe **nie powstrzymują złodzieja** – aktywują alarm i przesyłają wiadomość o nim np. do centrum monitorowania, które wysyła na miejsce zdarzenia patrol interwencyjny. To niestety nie powstrzymuje włamywacza, który często znika z łupem, zanim pojawią się odpowiednie służby.

Protect wprowadza obecnie trzecią generację generatorów dymu (a właściwie mgły). Pierwszą generację stanowiły urządzenia, które znają Państwo z koncertów i dyskotek. Ten podstawowy system jest wciąż wykorzystywany przez konkurencję, jednakże produkuje dym, którego gęstość jest o 67% mniejsza niż gęstość dymu generowanego przez nasz produkt. Generator dymu drugiej generacji to kolejny etap ewolucji. Koszt takiego systemu to zaledwie jedna trzecia ceny starszych urządzeń. Obudowa została zmodernizowana w taki sposób, że urządzenia stały się lżejsze i łatwiejsze w montażu. W zaledwie kilka godzin można zainstalować urządzenie, które w przypadku włamania ogranicza widoczność



do kilku centymetrów, a dodatkowy czujnik weryfikacyjny minimalizuje niemal do zera możliwość wystąpienia fałszywych alarmów.

Najnowszym innowacyjnym produktem firmy Protect jest przenośne urządzenie zamgławiające, sterowane telefonem komórkowym – **FOG Cannon SMS.**

Altana z drogimi narzędziami na działce, tymczasowy magazyn czy pomieszczenie badawcze wypełnione komputerami – wszystko to może teraz być objęte ochroną przenośnego urządzenia zamgławiającego Protect, sterowanego telefonem komórkowym poprzez komunikaty zawarte w treści wiadomości SMS. Urządzenie może być zastosowane bez ograniczeń wszędzie tam, gdzie tradycyjna instalacja systemu alarmowego jest niemożliwa lub nieopłacalna. Sterowanie urządzeniem odbywa się poprzez telefon komórkowy.

W wielu sytuacjach nie jest możliwe zainstalowanie tradycyjnego urządzenia zamgławiającego Protect jako elementu istniejącej instalacji alarmowej. Przykładem może być wprowadzenie się do nowego mieszkania czy biura, gdzie system alarmowy jest jeszcze niekompletny, a właściciel posiada tam już cenne rzeczy.

Właśnie dlatego Protect opracował nowe działko zamgławiające, które w łatwy i szybki sposób może być zainstalowane tam, gdzie konwencjonalne systemy alarmowe nie mogą być jeszcze zastosowane.

Wyrzut mgły pod ciśnieniem jest uruchamiany w momencie, gdy zintegrowany czujnik PIR wykryje i zasygnalizuje ruch w chronionej strefie. Dzięki obecnej w urządzeniu skrzynce GSM możliwa jest aktywacja i dezaktywacja urządzenia za pośrednictwem telefonu komórkowego. Wiadomość SMS informuje również o wszelkich zmianach ustawień.

– Opracowaliśmy nowe, „samodzielne" działko zamgławiające, ponieważ pojawiła się taka potrzeba rynkowa. Wielu klientów Protect posiada obiekty w trakcie budowy lub rekonstrukcji, które muszą być na ten okres odpowiednio zabezpieczone – do momentu zainstalowania właściwego systemu alarmowego – wyjaśnił Poul Dalsgaard, dyrektor zarządzający firmy Protect.

W praktyce mgła jest wyzwalana, gdy czujnik PIR zarejestruje ruch w chronionym obszarze. W tym samym czasie wiadomość SMS sygnalizuje alarm, a informacja ta może być wysłana do czterech osób.

Co więcej, wszelkie zmiany w ustawieniach urządzenia są przesyłane wiadomością SMS do użytkownika. Odbiorca jest informowany o aktywacji urządzenia, próbie sabotażu, niskim poziomie fluidu czy spadku napięcia. Każdorazowo, po usunięciu usterek, użytkownik otrzymuje wiadomość potwierdzającą gotowość urządzenia do ponownego użycia.

Utrudnić życie złodziejowi

Wiele sobie obiecujemy po nowym produkcie. Spełnia on oczekiwania naszych klientów dotyczące łatwości zastosowania, elastyczności miejsca montażu – tam, gdzie tradycyjny system jest trudny bądź niemożliwy do zastosowania. Będąc pewną zalet tego urządzenia, firma Protect opatentowała swój wyrób. Powtarzające się włamania z kradzieżami przysparzają wielu kłopotów właścicielom obiektów, pochłaniają czas i pieniądze. Mamy nadzieję, że, dzięki naszemu nowemu patentowi, utrudnimy życie złodziejom.

Duńska jakość

Mgła jest stosunkowo nowym sposobem zabezpieczania kosztowności. Od momentu założenia firmy Protect w 2001 roku ponad 10 000 systemów alarmowych zostało wyposażonych w działka zamgławiające. Urządzenia Protect znalazły szerokie zastosowanie w różnych miejscach, m.in. w urzędach, szkołach, zakładach jubilerskich, sklepach RTV i z telefonią komórkową, na stacjach benzynowych, w domach prywatnych. Działania Protect mają obecnie charakter globalny. Firma eksportuje swoje urządzenia do ponad 30 krajów, w tym do Polski. Ostatnio działalność została z sukcesem poszerzona i prowadzona jest w USA, Australii, Nowej Zelandii, Afryce Południowej i Europie Wschodniej.

Podstawowa oferta

Nadal w podstawowej ofercie firmy dostępne są modele urządzeń o wydajności 375, 550 i 1500 m^3, generowanej w czasie jednej minuty, oraz lampy stroboskopowe o mocy 2700 W, generujące do sześciu błysków na sekundę.

Promocja!!!
Informujemy, iż teraz,
na zamówione urządzenia
Protect
udzielamy rabatu w wysokości 20%.

Zapraszamy do skorzystania z urządzeń firmy Protect. Jesteśmy przekonani o skuteczności proponowanych zabezpieczeń dymnych (mgielnych). W razie pytań lub wątpliwości prosimy o kontakt.

Artur Zaborowski
AWC Protect Global System Polska
ul. Bema 87, 01-233 Warszawa
tel.: (022) 456 87 79, faks: (022) 456 87 84
e-mail: biuro@protectglobal.com.pl
www.protectglobal.com

Centralny monitoring

Nowoczesne zamki i nowatorskie oprogramowanie

Nasz partner, firma Kaba Mauer, jest czołowym producentem zamków wysokiego bezpieczeństwa (w skrócie HSL, od ang.: *High Security Lock*).

W swojej 140-letniej działalności łączy długoletnie doświadczenie w tej dziedzinie z najnowszymi technikami wytwarzania, dzięki czemu osiągnęła wysoką pozycję na rynku zabezpieczeń. Stosuje system jakości zgodny z DIN EN ISO 9001, co gwarantuje najlepszą jakość wyrobu.

Zamki Safe Lock 523 i Safe Lock 525 posiadają wiele funkcji zabezpieczających o dużym stopniu wyspecjalizowania. Umożliwiają programowanie różnych kodów i ich kombinacji oraz funkcji zależnych od czasu, a także zapamiętywanie zdarzeń i udostępnianie zapisanych informacji. Zamki Safe Lock przeznaczone są do:

– blokowania wszelkich mechanizmów ryglowych urządzeń wymagających wysokiego bezpieczeństwa,
– rejestracji zdarzeń zaistniałych podczas ich użytkowania.

Mogą być zastosowane do blokowania:

– wszelkiego typu drzwi,
– szaf,
– pomieszczeń,
– urządzeń, od których wymagamy wysokiego bezpieczeństwa użytkowania.

Zamki Safe Lock są szczególnie przydatne w przypadku eksploatacji urządzeń i obiektów, do których dostęp ma wielu użytkowników, lub przy często zmieniających się planach kontroli dostępu z pełną rejestracją zdarzeń. Kształt i wymiary zamków są typowe dla tej grupy urządzeń. Umożliwia to zastosowanie ich we wszelkich nowych urządzeniach i obiektach. Mogą być zastosowane zamiennie w urządzeniach już eksploatowanych, wyposażonych w inne zamki elektroniczne lub mechaniczne.

Cechą wyróżniającą zamki Safe Lock jest wyświetlacz, który ułatwia posługiwanie się urządzeniem i eliminuje konieczność zapamiętania związanej z tym procedury, co może stanowić problem w niektórych przypadkach. Na wyświetlaczu widoczne są informacje o stanie zamka i kolejnych krokach, które musi wykonać użytkownik.

Do pamięci zamka można wczytać 18 kodów użytkowników, podporządkowanych odpowiednim kodom *master*.

Każdemu użytkownikowi można przydzielić czas, zgodny z kalendarzem tygodniowym, w którym będzie mógł mieć dostęp do swojego kodu i dokonać otwarcia zamka. Wszystkie zdarzenia będą zapisane w pamięci urządzenia.

Kolejną cechą wyróżniającą opisywane zamki jest możliwość odczytu zdarzeń przy pomocy standardowego komputera z odpowiednim oprogramowaniem. **Nie trzeba zaopatrywać się w dodatkowe wyposażenie, umożliwiające odczyt pamięci zamka.**

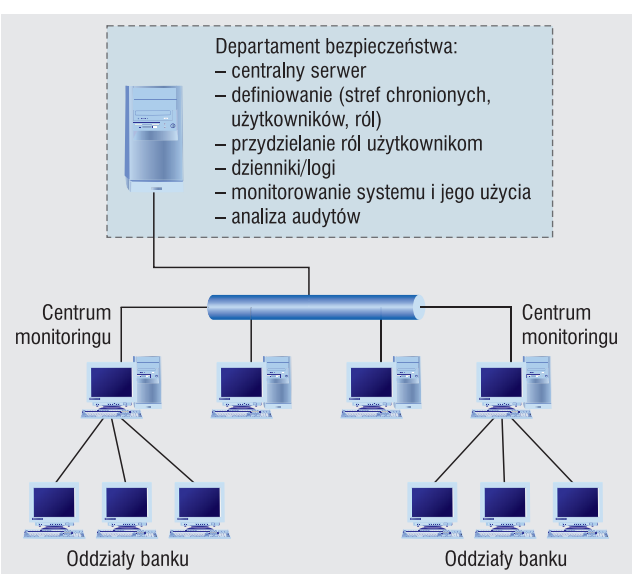
Zamki Safe Lock mogą działać w centralnym systemie kontroli dostępu i monitoringu obiektów i urządzeń.

Obecnie większość banków w Polsce o dużej sieci jednostek organizacyjnych, przy dostępie pracowników, firm konwojowych oraz serwisantów do obiektów i urządzeń szczególnie chronionych przez nieuprawnionym dostępem, stosuje:

– lokalne nadawanie dostępu do stref chronionych,
– lokalne odbieranie uprawnień,
– przekazywanie kluczy mechanicznych,
– dokumentowanie przyznanych uprawnień,
– okresowe audyty.

Te rozproszone czynności mogą być scentralizowane dzięki zastosowaniu zamków elektronicznych, np. firmy Mauer, oraz zastosowaniu odpowiedniego oprogramowania, np. firmy Kłos Software. Całością zarządzania dostępem do obiektów i urządzeń szczególnie chronionych mogłoby zajmować się Centrum Monitoringu, zlokalizowane np. w Departamencie Bezpieczeństwa, w którym znajduje się centralny serwer, odpowiedzialnym za:

– definiowanie (stref chronionych, użytkowników, ról),
– przydzielanie ról użytkownikom,
– dzienniki/logi,
– monitorowanie systemu i jego użycia,
– analizę audytów.



Wszystkie firmy i osoby zainteresowane tematem zamków wysokiego bezpieczeństwa zapraszamy do bezpośredniego kontaktu. Będzie nam bardzo miło zaprosić Państwa do naszej siedziby lub przyjechać do Państwa.

Zbigniew Kłos

Zbigniew Kłos, producent zamków i urządzeń bankowych
Mościska 26A, 05-080 Izabelin k. Warszawy, tel. (0-22) 722-86-90
http://www.klos.com.pl

KŁOS Software
tel. (0-22) 721-80-90 http://www.klossoftware.pl

Ciągłość działania i odtwarzanie po awarii (BC/DR) w kontroli ruchu lotniczego. Część 2.

Aktualne procedury i standardy w świetle nowych tendencji standaryzacyjnych

Niniejszy artykuł to część druga cyklu na temat ciągłości działania i odtwarzania po awarii (BC/DR, z ang.: ***Business Continuity/Disaster Recovery***) w kontroli ruchu lotniczego. Na początku zostanie zaprezentowana historia powstawania standardów dotyczących BC/DR, ich powiązania z już istniejącymi normami ISO/IEC i nie tylko. Następnie będą pokrótce przedstawione zasady tworzenia planów BC/DR, ich wdrażania, testowania, aktywacji i dezaktywacji oraz przykładowe sposoby oceny efektywności tych planów. Po krótkim przeglądzie jednej z proponowanych norm zostaną omówione aktualne akty prawne, normujące bezpieczne prowadzenie kontroli ruchu lotniczego, będące regulacjami zarówno międzynarodowymi jak i krajowymi. Następnie w skrócie opisane będą zagrożenia dla ruchu lotniczego oraz aktualne procedury mające za zadanie ograniczenie zakresu oraz likwidację skutków zdarzeń niepożądanych (awarii, celowych uszkodzeń, ataków terrorystycznych itp.). Na zakończenie zostaną podane aktualne informacje na temat wykorzystania procedur BC/DR w kontroli ruchu lotniczego, w świetle wcześniej omówionych standardów

Geneza standardów BC/DR

Obecnie prowadzenie jakiejkolwiek działalności gospodarczej jest niemożliwe bez wykorzystania najnowszych technologii w dziedzinie telekomunikacji i informatyki. To ścisłe powiązanie ujawnia się szczególnie mocno w przypadku wszelkiego rodzaju awarii spowodowanych przez złą obsługę, włamania do systemów, katastrofy naturalne lub ataki terrorystyczne. Wielokrotnie okazywało się, że nawet duże firmy nie były przygotowane na takie ewentualności, co z kolei prowadziło do ograniczenia ich działalności a nierzadko do całkowitego zniknięcia z rynku w sytuacjach awaryjnych. Doświadczenia te wymusiły na wielu instytucjach uwzględnianie w swoich planach działania specjalnych procedur, które mogłyby uchronić je przed tragicznymi skutkami katastrof i awarii.

Początkowo zadowalano się budowaniem systemów z wszelkiego rodzaju nadmiarowością (dyski, pamięci, procesory a nawet całe systemy komputerowe) w jednym ośrodku przetwarzania. Jednak już wkrótce okazało się, że takie podejście w wielu przypadkach jest niewystarczające. Rozpoczęto więc prace nad budową zapasowych centrów przetwarzania. Prace te były jednak początkowo bardzo utrudnione ze względu na brak jakichkolwiek doświadczeń w tej dziedzinie, a co za tym idzie – brak krajowych i międzynarodowych norm. Co prawda powstawały instytucje, takie jak *Disaster Recovery Institute* (DRI) [28] lub *Business Continuity Institute* (BCI) [29], zajmujące się certyfikacją i edukacją w dziedzinie BC/DR, ale to nie rozwiązywało problemu w skali globalnej.

Jednym z impulsów do opracowania normy międzynarodowej było wydanie w Singapurze w 2004 roku normy dotyczącej procedur BC/DR pt. *Business continuity/disaster recovery (BC/DR) service providers* [2]. Opisuje ona zasady budowy i utrzymania w działaniu zapasowych centrów przetwarzania informacji. Stosunkowo szybko, bo już w 2005 roku, połączony komitet ISO/IEC JTC 1/SC 27 rozpoczął prace nad międzynarodową normą zatytułowaną roboczo *Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services* [1]. Punktem wyjścia do jej opracowania stał się standard opracowany w Singapurze. W grudniu 2006 roku komitet ISO/IEC wydał

wersje FCD (*Final Committee Draft*), co oznacza, że już wkrótce norma ta powinna być opublikowana.

Jednocześnie należy zaznaczyć, że wiele krajów prowadziło lub prowadzi prace nad własnymi normami dotyczącymi BC/DR. Między innym w Stanach Zjednoczonych opracowany został w 2002 roku standard zatytułowany *Contingency planning guide for information technology systems* [3], a w Wielkiej Brytanii opublikowano dwuczęściowy standard BS 25999 [4,5].

Charakterystyka nowego standardu ISO/IEC

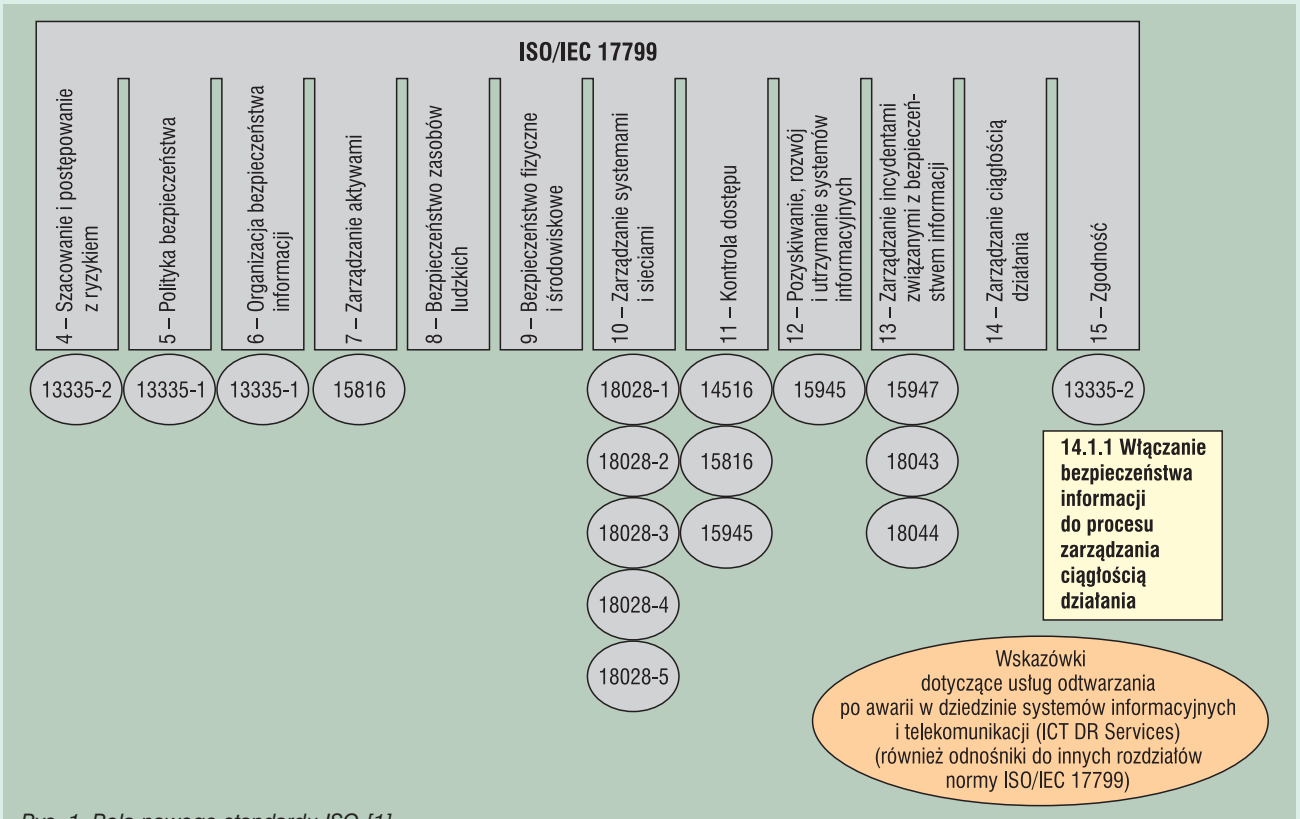
Nowy standard ISO dotyczący BC/DR powstaje jako element, który stanowi uzupełnienie już istniejących norm, a w szczególności normy ISO/IEC 17799.

Jak pokazano to na rys. 1, łączy się on bardzo ściśle z rozdziałem czternastym wyżej wymienionego standardu, aczkolwiek występują też odwołania do innych rozdziałów.

Standard ten opiera się na strukturze wielowarstwowej, zawierającej różne elementy, które są niezbędne do zapewnienia szeroko pojętych usług odtwarzania po awarii dla technologii informacyjno-komunikacyjnych (ICT DR – od ang. *Information and Communication Technology Disaster Recovery*). Podstawę tej struktury (rys. 2) stanowią polityki (*Policies*), ocena efektywności (*Performance Measurement*), procesy (*Process*) oraz ludzie (*People*). Warstwy te pomagają zdefiniować infrastrukturę (*Infrastructure*) zapewniającą odtwarzanie po awarii oraz zakres świadczonych usług (*Services Capability*). Ciągłe ulepszanie (*Continuous improvement*) umożliwia wybór najlepszych rozwiązań w poszczególnych dziedzinach tej działalności oraz podnosi poziom usług. Tak więc wszystkie wskazówki zawarte w tym standardzie biorą się z całościowego spojrzenia na niniejszą strukturę oraz zapewniają równowagę pomiędzy ponoszonymi kosztami a odpowiednim poziomem świadczonych usług [1].

Polityki umożliwiają dostawcy usług ICT DR (rozumianemu jako dostawca wewnętrzny lub zewnętrzny) określenie kierunków działania w obszarach powiązanych ze świadczeniem usług ICT DR oraz umożliwiają łatwą i szybką komunikację, zgodną z ustanowionymi regułami, z wszystkimi podmiotami zaangażowanymi w proces ich świadczenia (klientami oraz dostawcami). Dzięki ocenie efektywności możliwa jest bieżąca kontrola oraz poprawa poziomu usług, a to z kolei umożliwia dostawcy usług ICT DR zapewnienie swoich klientów, że usługi są świadczone na najwyższym możliwym poziomie. Procesy zapewniają spójne podejście do zagadnień niezwiązanych bezpośrednio ze świadczeniem usług ICT DR, umożliwiając w ten sposób ciągłe utrzymanie poziomu usług oraz ułatwiając szkolenie personelu. Wszystkie wyżej wymienione elementy nie są możliwe do zrealizowania bez odpowiednio przygotowanego i wyszkolonego personelu. Dotyczy to zarówno osób zaangażowanych bezpośrednio w świadczenie usług ICT DR oraz innych pracowników, którzy w jakikolwiek sposób mają wpływ na jakość tych usług (np. firm zewnętrznych). Ponadto bardzo istotnym elementem, który należy zawsze brać pod uwagę w tego typu działalności, jest potrzeba zapewnienia bezpieczeństwa i opieki wszystkim osobom odpowiedzialnym w jakikolwiek sposób za świadczenie usług ICT DR [1].

Każdy dostawca usług ICT DR powinien dokładnie rozpoznać swoje potrzeby związane z zapewnieniem ciągłości działania oraz odtwarzaniem po awarii. Ostatecznym celem dla każdego dostawcy takich usług jest opracowanie planu



Rys. 1. Rola nowego standardu ISO [1]

zapewniającego ciągłość działania, przetestowanie go, a następnie dostosowywanie go do zmieniających się funkcji biznesowych. Dostawca nie powinien jednak przystępować bezpośrednio do tworzenia odpowiednich planów, lecz wykonać wcześniej kilka niezbędnych kroków. Prace należy rozpocząć od zidentyfikowania priorytetów, a następnie dobrać poprawną i najbardziej efektywną strategię zapewnienia ciągłości działania dla swojego środowiska biznesowego. Dopiero po dokonaniu takiej oceny można przystąpić do opracowywania odpowiednich planów. Ponadto należy wdrożyć procedury ograniczania ryzyka, które mają za zadanie ograniczyć prawdopodobieństwo wystąpienia sytuacji, w której należałoby uruchomić plany BC/DR oraz ograniczać skutki ewentualnych katastrof i awarii.

Ogólny schemat działania przedstawiono na rys. 3. Zalecane postępowanie obejmuje kilka kroków dobranych w taki sposób, aby w wyniku ich wykonania został opracowany wszechstronny i wykonalny plan zapewnienia ciągłości działania. Ma on spełniać wszystkie niezbędne wymagania stawiane przez dostawcę usług ICT DR w przypadku wystąpienia katastrofy lub awarii. Schemat ten zawiera [1]:

- ocenę priorytetów podczas odtwarzania (DR), ram czasowych oraz minimalnych wymogów (łącznie z analizą wpływu zdarzenia na prowadzoną działalność),
- określenie strategii w dziedzinie zapewnienia ciągłości działania (BC),
- opracowanie planu BC,
- testowanie planu BC,
- szkolenie załogi z zakresu BC,
- bieżące „utrzymanie" planu BC,
- ograniczanie ryzyka.

Pierwsze pięć kroków wykonywanych jest kolejno. Po opracowaniu planu BC krok szósty wykonywany jest cyklicznie lub po pojawieniu się zmian, które mogą mieć wpływ na realizację planu. W tym celu należy cofnąć się do wcześniejszych kroków tak, aby można było uwzględnić zmiany, które wpływają na plan BC. Krok siódmy wykonywany jest równolegle w trakcie wykonywania wszystkich pozostałych kroków [1].

Jeżeli usługi DR są świadczone przez zewnętrznego dostawcę, powinien on wykonać podobne planowanie, jak w przypadku opisanym wcześniej, tylko w dziedzinie DR. Proces ten został zilustrowany na rys. 4.

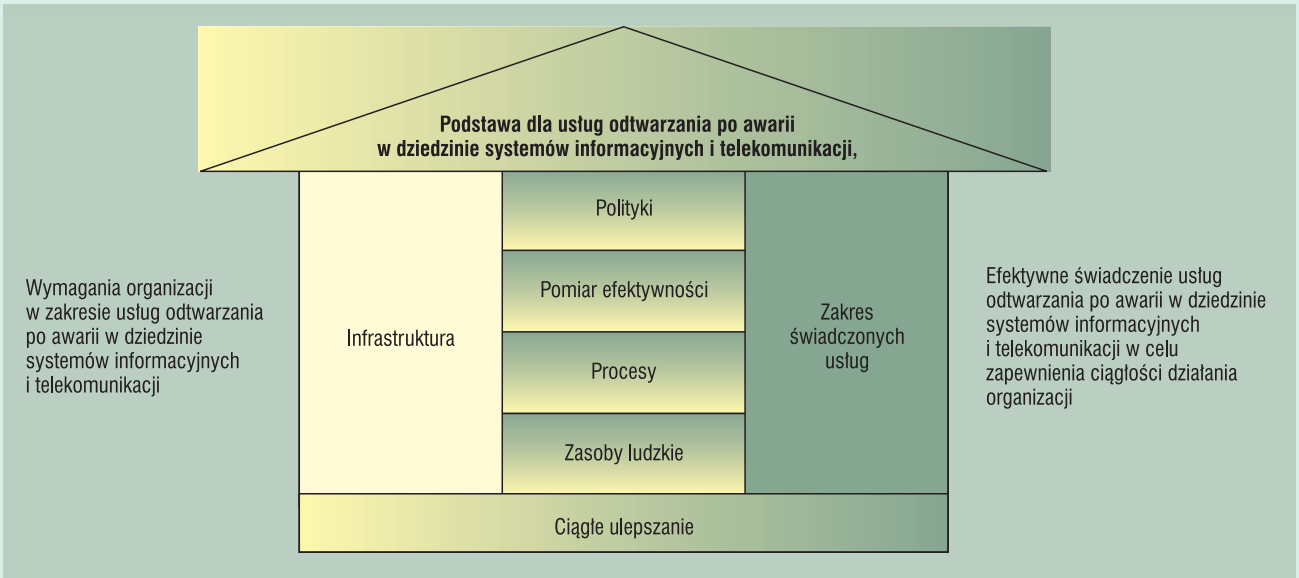
Oprócz wytycznych dotyczących planowania BC/DR określono dość dokładnie wymogi, jakie powinny zostać postawione zapasowym ośrodkom przetwarzania informacji. Dotyczą one między innymi:

- lokalizacji zapasowych centrów przetwarzania,
- infrastruktury,
- poziomów i typów usług,
- planów aktywacji/dezaktywacji procedur DR,
- doboru załogi,
- szkolenia,
- testowania,
- pomiaru efektywności,
- skalowalności.

Szerszego omówienia wymaga pomiar efektywności. Pozwala on dostawcom usług ICT DR ocenić między innymi jakość świadczonych usług, wpływ katastrofy lub awarii na dostępność do informacji i infrastruktury, a co za tym idzie – wpływ na prowadzoną działalność i ryzyko z tym związane. Daje także możliwość zademonstrowania klientom potencjalnych zdolności do odtworzenia po wystąpieniu krytycznego zdarzenia. Dzięki pomiarowi efektywności możemy oceniać postęp w jakości świadczonych usług ICT DR oraz dokonywać porównań pomiędzy poszczególnymi dostawcami usług [1].

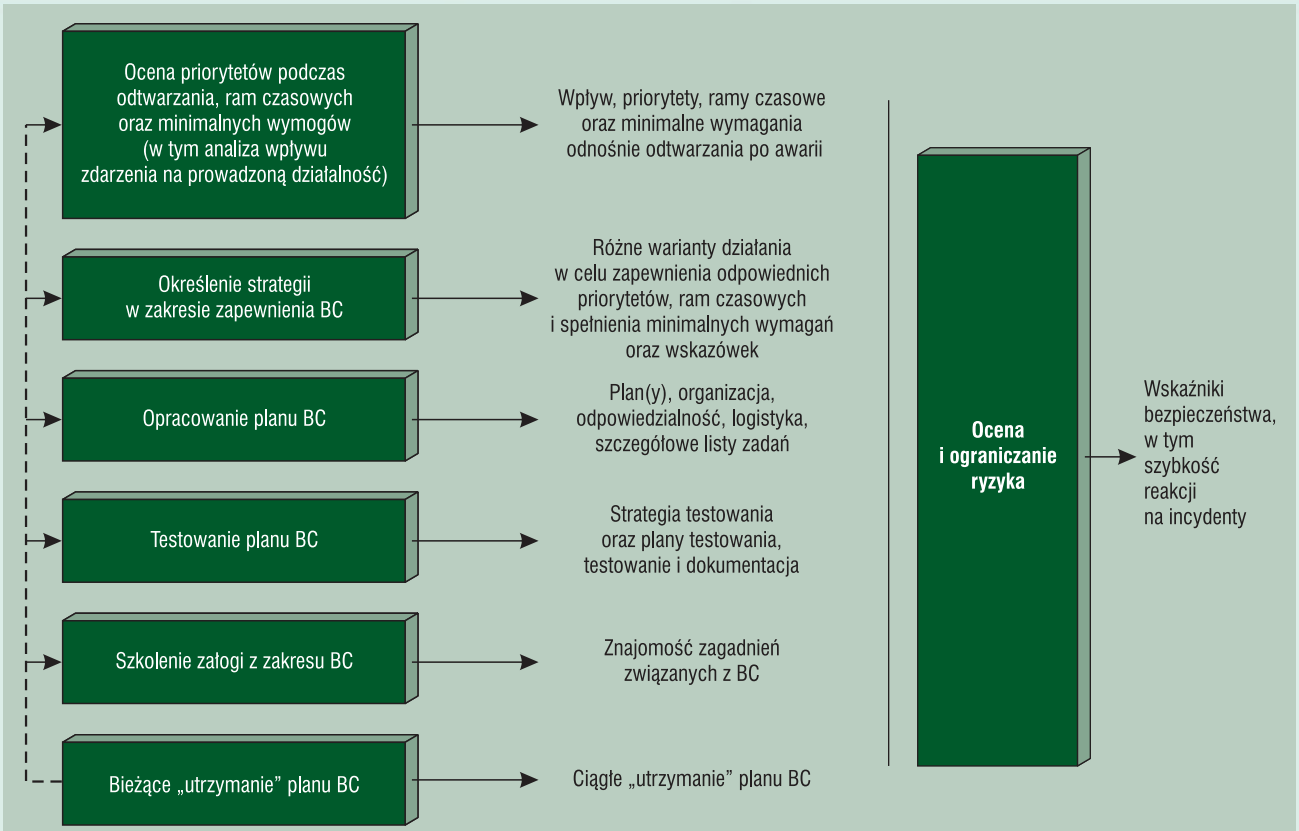
Wybór wskaźników efektywności oraz ich liczba będzie zależeć od wymagań stawianych przez daną organizację. Jako przykład można podać tutaj liczbę osób, które zostały przeszkolone w zakresie ICT DR, procent sprzętu lub zapasowych ośrodków przetwarzania informacji będących w ciągłym utrzymaniu lub stopień zgodności z niniejszym standardem [1].

W tym miejscu należy podkreślić, że chociaż nowy standard ISO/IEC jest w końcowej fazie opracowywania, to jego niektóre fragmenty mogą jeszcze ulec zmianie, dlatego też zaleca się traktowanie go jako wersji roboczej, a nie wersji finalnej, w której wszystkie elementy są precyzyjnie zdefiniowane. ➨



Rys. 2. Wielowarstwowy model dla usług odtwarzania po awarii w dziedzinie systemów informacyjnych i telekomunikacji (ICT DR Framework) [1]


Centrum Monitorowania Alarmów sp. z o.o.
Życzy wszystkim czytelnikom
Automonitoring GPS
W Święta Bożego Narodzenia
odpoczynku od codzienności,
a w Nowym 2008 Roku
energii do realizacji śmiałych zamierzeń
Multimonitoring
www.cma.com.pl



Rys. 3. Planowanie w zakresie zapewnienia ciągłości działania (BC) [1]

Niniejsza krótka charakterystyka nowego standardu pokazuje, jak trudne i kosztowne w realizacji mogą być rozwiązania zapewniające ciągłość działania oraz umożliwiające odtworzenie po katastrofie lub awarii. Pomimo to coraz więcej organizacji planuje wdrożenie lub już wdraża plany BC/DR. Jedną z dziedzin, w której zagadnienia związane z BC/DR są stawiane od początku na ważnym, jeśli nie na pierwszym, miejscu, jest kontrola ruchu lotniczego. Jej zadaniem jest, przypomnijmy, zapewnienie bezpiecznej separacji pomiędzy statkami powietrznymi zarówno w powietrzu, jak i na lądzie, przy jednoczesnym zapewnieniu jak najbardziej efektywnych warunków operacyjnych oraz ekonomicznych. W związku z tym już od dawna stosowane są w tej dziedzinie różnego rodzaju bardziej lub mniej zaawansowane plany BC/DR.

BC/DR w kontroli ruchu lotniczego – aktualne procedury i standardy

Jednym z najważniejszych narzędzi używanych w kontroli ruchu lotniczego jest radiowa komunikacja głosowa pomiędzy statkiem powietrznym a ośrodkiem kontroli (G/A). Bez niej nie jest możliwe prowadzenie sprawnej kontroli i zapewnienie bezpiecznej separacji pomiędzy samolotami. Dlatego też w przypadku awarii urządzeń łączności G/A dany fragment przestrzeni jest zamykany dla ruchu, a wszystkie statki, które się w nim znajdowały w trakcie jej wystąpienia, są przekazywane najszybciej, jak to możliwe, do sąsiednich ośrodków kontroli. Drugim ważnym elementem, który należy brać pod uwagę, jest czynnik ludzki. Kontrolerzy, bo o nich tu mowa, powinni zostać wyszkoleni na najwyższym możliwym poziomie i być w dobrym stanie zdrowia fizycznego i psychicznego. Posiadają oni status licencjonowanego personelu lotniczego, a zatem są bardzo trudni do zastąpienia na swoich stanowiskach. Sprawę komplikuje fakt, że do wyszkolenia samodzielnego kontrolera potrzeba minimum dwóch lat. Możliwość wymiany kontrolerów pomiędzy ośrodkami jest mocno utrudniona, ponieważ są oni przygotowywani do pracy na konkretnym stanowisku, a nierzadko do kontrolowania ściśle wyznaczonego obszaru. Innymi elementami, które należy brać pod uwagę podczas planowania BC/DR, są przerwy w łączności pomiędzy ośrodkami (G/G), przerwy w działaniu systemu radarowego, brak dostępu do systemu przetwarzania planów lotów, zaniki zasilania oraz uszkodzenia pomocy nawigacyjnych. Nie należy też ignorować takich zagrożeń, jak ataki terrorystyczne i katastrofy naturalne, które mogą prowadzić nawet do całkowitego zniszczenia ośrodków kontroli.

Aktualnie planowanie BC/DR (inaczej zwane „contingency") w kontroli ruchu lotniczego skupia się najczęściej na ograniczaniu skutków katastrofy lub awarii. Najczęściej składa się ono z następujących etapów:

- redukcji pojemności lub całkowitego zamknięcia FIR/sektora,
- uruchomienia zapasowych systemów komunikacyjnych oraz zapasowych systemów informatycznych,
- odtworzenia po awarii,
- przywrócenia pełnej pojemności FIR/sektora.

Z reguły tego typu plany BC/DR są przygotowywane lokalnie i obejmują w większości przypadków jeden ośrodek kontroli obszaru (ACC). Na dzień dzisiejszy tylko kilka krajów posiada wzajemną rezerwację dwóch lub więcej centrów operacyjnych. Jednym z nich jest Irlandia. Według dostępnych

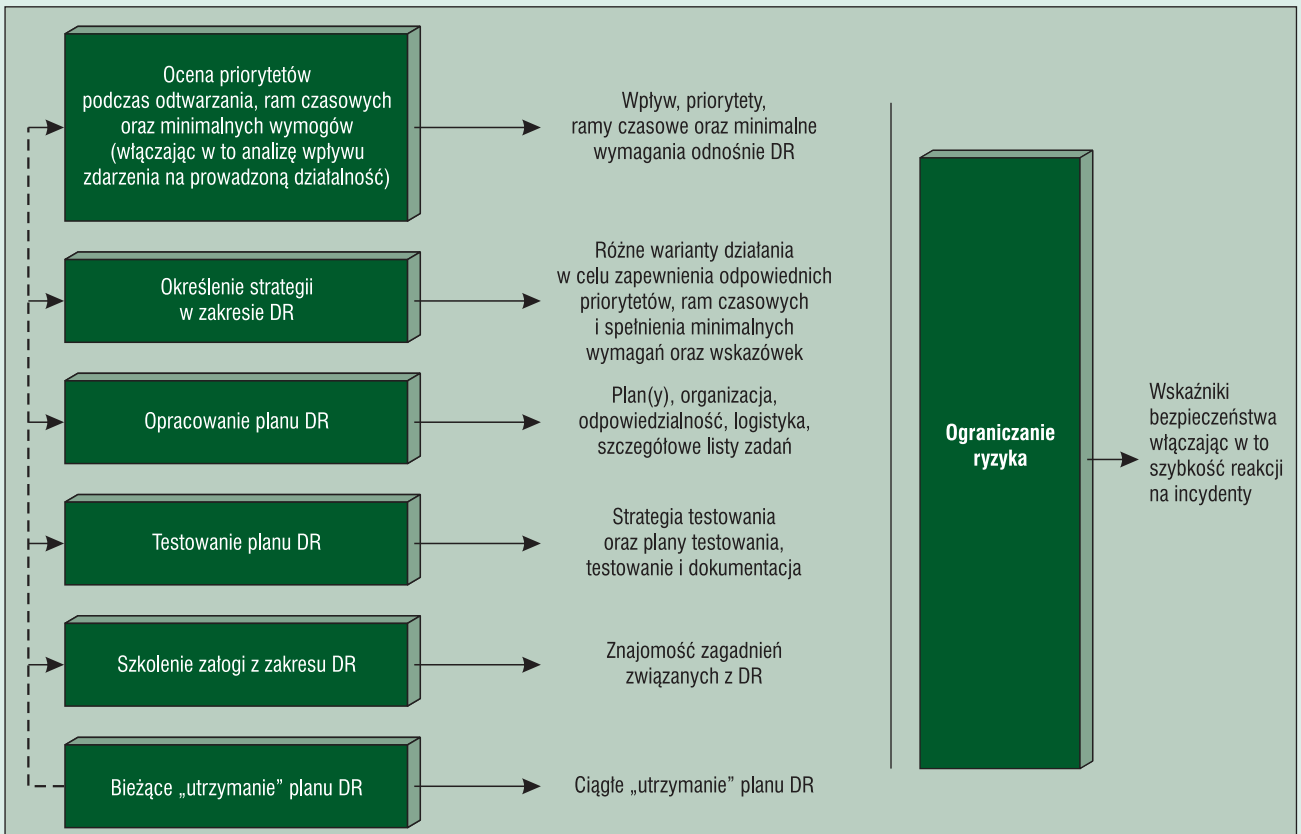
informacji dwa nowoczesne ośrodki w Dublinie oraz Shannon, należące do Irish Aviation Authority (IAA), posiadają wspólne plany „contingency" [18]. Powstały też projekty współpracy kilku krajów w dziedzinie BC/DR. Jednym z nich jest NUAC (*Nordic Upper Area Control Center*) [20]. Projekt ten obejmuje swoim zasięgiem Danię, Finlandię, Norwegię oraz Szwecję. Aktualnie istnieje kilka ściśle współpracujących ze sobą ośrodków, posiadających odpowiednie plany zapewnienia ciągłości działania oraz odtwarzania po katastrofie lub awarii. Istnieje też duże prawdopodobieństwo, że Szwajcaria, Niemcy oraz Austria mają podpisaną umowę o współpracy w dziedzinie planów BC/DR. Brak jest natomiast jakichkolwiek informacji na temat współpracy ośrodków kontroli w takich krajach, jak Stany Zjednoczone (kilkadziesiąt ośrodków), Kanada (siedem ośrodków kontroli obszaru) oraz Australia (dwa nowoczesne środki kontroli w Brisbane i Melbourne). W Europie jeden z największych międzynarodowych projektów w dziedzinie kontroli ruchu lotniczego, jakim jest MUAC (*Maastricht Upper Area Control Centre*), jest realizowany tylko i wyłącznie w jednym ośrodku kontroli. Aktualnie nic nie wiadomo na temat szerszej współpracy w dziedzinie planów BC/DR pomiędzy tym centrum kontroli a innymi ośrodkami znajdującymi się w krajach ościennych. W Polsce na dzień dzisiejszy istnieje tylko jeden ośrodek kontroli obszaru, który powstał z połączenia na przełomie wieków dwóch ośrodków działających w Warszawie i w Poznaniu, a co za tym idzie – brakuje wzajemnej rezerwacji pomiędzy centrami kontroli. W tym miejscu należy zaznaczyć, że wszystkie wyżej opisane plany BC/DR obejmują swoim zasięgiem tylko i wyłącznie ośrodki kontroli obszaru. Nie są znane rozwiązania, które zapewniałyby wzajemną rezerwację dla ośrodków kontroli zbliżania oraz kontroli lotniska.

Aktualnie wszystkie aspekty związane z bezpieczeństwem w kontroli ruchu lotniczego są opisane w aneksach ICAO oraz odpowiednich dokumentach (DOC), wydanych przez tę organizację. Obowiązują one (z wyjątkami) kraje przynależące do ICAO, w tym Polskę. W Europie dodatkowe regulacje zostały wydane przez EUROCONTROL i znane są jako *pan-European Safety Regulatory Requirements* (ESARR) [19]. Polska, na mocy Rozporządzenia Ministra Infrastruktury z dnia 5 października 2004 r. (Dz.U. Nr 224/2004, poz. 2283) przyjęła za obowiązujące następujące dokumenty:

- ESARR 2 – Składanie meldunków oraz rozpatrywanie nieprawidłowości w ruchu lotniczym (*Reporting and Assessment of Safety Occurrences in ATM*),
- ESARR 3 – Wykorzystanie systemów zarządzania bezpieczeństwem przez organy zarządzania ruchem lotniczym (*Use of Safety Management Systems by ATM Service Providers*),
- ESARR 4 – Ocena i ograniczanie ryzyka w systemie zarządzania ruchem lotniczym (*Risk Assessment and Mitigation in ATM*),
- ESARR 5 – Personel służb zarządzania ruchem lotniczym (*ATM Services' Personnel*).

Wyżej wymienione dokumenty nie obejmują jednak procedur BC/DR w rozumieniu takim, jakie zostało przedstawione na początku niniejszego artykułu.

Problem BC/DR, ujmowany z perspektywy międzynarodowej, nie jest prosty. Pomimo istnienia wielu ścisłych przepisów,



Rys. 4. Planowanie w zakresie odtwarzania po awarii (DR) [1]

wytycznych oraz standardów, kontrola ruchu lotniczego przebiega w każdym kraju inaczej. Różnice nie dotyczą tylko sprzętu, oprogramowania, procedur, ale także tak istotnych elementów, jak podział przestrzeni powietrznej. O ile planowanie BC/DR w ramach jednego państwa jest możliwe do zrealizowania, o tyle w skali międzynarodowej jest to ogromne wyzwanie. Na tak wysokim poziomie oprócz problemów *stricte* technicznych i organizacyjnych do głosu dochodzą kwestie polityczne, wojskowe oraz ogólnie pojętego bezpieczeństwa państwa. W aktualnej sytuacji międzynarodowej nie można tych problemów ignorować lub uznawać ich za nierozwiązywalne. W dobie szybko postępującej globalizacji oraz coraz szybszego nasycania kontroli ruchu lotniczego zaawansowaną technologią może okazać się, że niektóre państwa są skazane na współpracę międzynarodową w zakresie planowania BC/DR. Dlatego też należy dążyć do ujednolicania niezbędnych przepisów, procedur i wielu innych elementów kontroli ruchu lotniczego tak, aby w przyszłości było możliwe nawiązywanie współpracy w tej dziedzinie na płaszczyźnie międzynarodowej.

Aktualnie organizacja Eurocontrol powołała specjalną grupę roboczą, która ma się zająć planowaniem BC/DR. W ramach prac przewidziane jest opracowanie wytycznych dla planów odtwarzania po wystąpieniu katastrofy lub awarii. Nic nie wskazuje jednak na to, że w celu zapewnienia ciągłości działania będą tworzone oddzielne ośrodki kontroli, utrzymywane w pogotowiu, tak jak to jest proponowane w nowym standardzie ISO. Najprawdopodobniej zostanie wybrane rozwiązanie podobne do tych stosowanych już przez niektóre kraje, a opisywanych wcześniej w ramach niniejszego opracowania. Głównym powodem wyboru takiego rozwiązania może być potrzeba utrzymania możliwie najniższych kosztów funkcjonowania ośrodków kontroli ruchu lotniczego oraz wymóg bardzo dobrej znajomości przez kontrolerów stanowiska, na którym pracują. Wiąże się to z potrzebą ciągłej pracy na wybranym stanowisku i stałego podnoszenia swoich kwalifikacji. Dlatego właśnie ośrodki oczekujące w gotowości nie spełniłyby swojej roli, generując tylko wysokie koszty.

Podsumowanie

Duży nacisk, jaki jest położony w kontroli ruchu lotniczego na zapewnienie bezpieczeństwa, wymaga zaangażowania dużych środków technicznych oraz zasobów ludzkich. Wieloletnie doświadczenia pokazały jednak, że bez dobrych planów BC/DR nawet najlepszy ośrodek nie jest w stanie zapewnić ciągłości ruchu lotniczego w przypadku katastrofy lub awarii. Z tego powodu na dzień dzisiejszy większość istniejących centrów kontroli ma opracowane lokalne procedury awaryjne. Jednakże w obliczu postępującej globalizacji i szybkiego rozwoju technicznego i te zabezpieczania mogą okazać się zbyt słabe. Dlatego też coraz więcej ośrodków dostrzega potrzebę opracowania szerszych planów BC/DR, obejmujących swoim zasięgiem kraj lub nawet kilka krajów. Pomocne mogą okazać się prace nowego komitetu w ramach Eurocontrol, a także nowy standard ISO, który ma pojawić się już wkrótce.

Podziękowania

Pragnę podziękować Panu prof. Zbigniewowi Kotulskiemu, dr Ryszardowi Kossowskiemu, mgr inż. Maciejowi Rodakowi, mgr Jackowi Tomczakowi-Janowskiemu oraz mgr Marcinowi Wilkowskiemu za udzielenie pomocy przy opracowywaniu niniejszego artykułu. Bez ich wsparcia praca ta nie byłaby możliwa do zrealizowania.

Daniel Kiper
Instytut Telekomunikacji
Wydzia Elektroniki i Technik Informacyjnych
Politechniki Warszawskiej

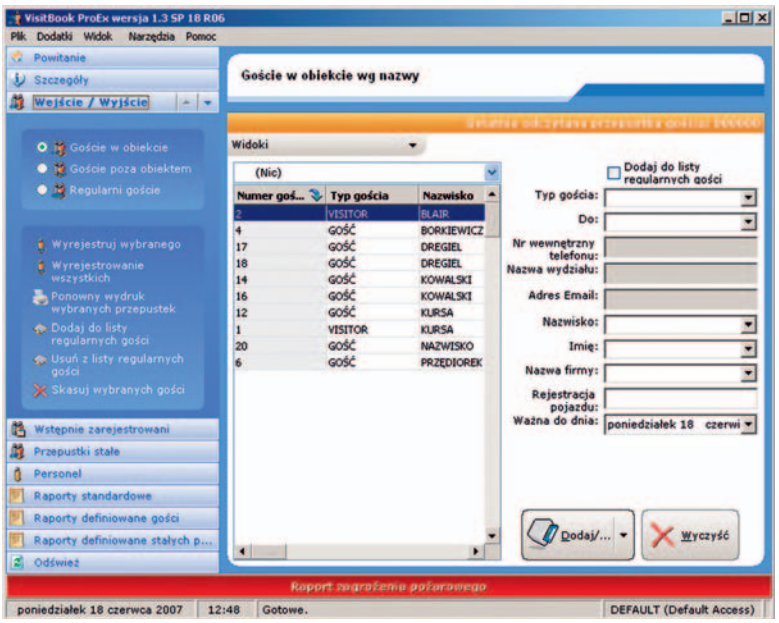
Zdjęcia:
Marcin Wilkowski

Literatura

[1] *Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services,* ISO/IEC FCD 24762, 2006-12-21.
[2] *SS 507:2004 – Business continuity/disaster recovery (BC/DR) service providers,* Singapore Standard, 2004.
[3] *SP 800-34 – Contingency Planning Guide for Information Technology Systems,* NIST, June 2002.
[4] *BS 25999-1:2006 Code of practice for business continuity management,* BSI, November 2006.
[5] *BS 25999-2:2007 Specification for business continuity management,* BSI, Spring 2007.
[6] A. Białas: *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,* WNT, Warszawa, 2006.
[7] Annex 2 to the Convention on International Civil Aviation, Rules of the Air, ICAO, Tenth Edition, July 2005.
[8] *Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Volume II Communication Procedures including those with PANS status,* ICAO, Sixth Edition, October 2001.
[9] *Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Volume III Communication Systems,* ICAO, First Edition, July 1995.
[10] *Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Volume IV Surveillance Radar and Collision Avoidance Systems,* ICAO, Third Edition, July 2002.
[11] *Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Volume V Aeronautical Radio Frequency Spectrum Utilization,* ICAO, Second Edition, July 2001.
[12] *Annex 11 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Air Traffic Services,* ICAO, Thirteenth Edition, July 2001.
[13] *Doc 4444, Air Traffic Management,* ICAO, Fourteenth Edition, 2001.
[14] *General & CFMU Systems,* EUROCONTROL, Edition 11.0, 02 May 2006.
[15] http://www.pansa.pl.
[16] http://www.icao.int.
[17] http://www.nga.mil.
[18] http://www.iaa.ie.
[19] http://www.eurocontrol.int/src/public/standard_page/src_deliverables.html.
[20] http://www.naviair.dk/page119.aspx?newsid119=104.
[21] http://en.wikipedia.org/wiki/Air_traffic_control.
[22] http://www.drii.org.
[23] http://www.thebci.org.

System rejestracji gości VisitBook

System rejestracji gości VisitBook jest narzędziem służącym do wspomagania pracy recepcji. Zastępuje papierową księgę gości jej elektronicznym odpowiednikiem. System umożliwia rejestrację danych gości 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 przez użycie czytnika kodów kreskowych. Program VisitBook został stworzony w trzech wersjach: Lite, Pro i ProEx.



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.

Ostatnia z nich – wersja ProEx jest wersją najbardziej rozbudowaną. Umożliwia ona wydruk przepustki wraz ze zdjęciem oraz zawiera między innymi funkcję projektowania własnych wzorów przepustek. Wydruk przepustek możliwy jest na standardowych drukarkach biurowych oraz drukarkach termosublimacyjnych do kart PVC (tylko wersja ProEx).

Zasadniczą zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program dodatkowo zawiera kilka użytecznych funkcji takich jak: manager personelu, manager kontrahentów, obsługa konferencji.

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

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 022 832 47 44, faks 022 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl

Rio2e i Tango2e drukują i zabezpieczają identyfikatory

MAGICARD

Profesjonalna drukarka zaprojektowana do seryjnego wydruku identyfikatorów.

Niezawodna oraz szybka i łatwa w obsłudze. Opatentowane rozwiązanie bezpieczeństwa HoloKote™ zabezpiecza karty przed nieautoryzowanym kopiowaniem.

Standardowo, podczas procesu wydruku karta pokrywana jest cienką folią (overlay) zabezpieczającą nadruk przed uszkodzeniem mechanicznym.

Wbudowana funkcja HoloKote™ umożliwia naniesienie na folii zabezpieczającej znaku wodnego (standardowo 2 wzory do wyboru).

Użycie opcjonalnej karty zabezpieczającej umożliwia nadruk znaku wodnego zawierającego tekst lub logo firmy. Karta taka może również spełniać funkcję klucza zabezpieczającego przed nieautoryzowanym użyciem drukarki.

Rio2e i Tango2e wyposażone są w wyświetlacz LCD informujący o statusie drukarki.

Drukarki posiadają certyfikat CE.

Holokate™ – znak wodny drukowany na całej powierzchni karty. Widoczny przy patrzeniu pod kątem.

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

Nadruk od krawędzi do krawędzi. Nadruk z jakością 300 dpi na całej powierzchni karty.

Interfejs Ethernet

Dwustronny nadruk – tylko drukarka Tango2e

3 lata gwarancji (łącznie z głowicą). Możliwość przedłużenia gwarancji do 4 lat.

Opcje:

Dowolna grafika lub tekst w znaku wodnym.

Możliwość kodowania kart magnetycznych.

Możliwość kodowania kart chipowych i zbliżeniowych.

SPECYFIKACJA TECHNICZNA
Prędkość nadruku
Wydruk karty w kolorze w 22 s
Wydruk karty monochromatycznej w 6 s
Wbudowane zabezpieczenia
HoloKote anti-coping – znak wodny na całej powierzchni karty
Typy taśm
LC1: YMCKO 350 wydruków
LC3 : Monochromatyczna 1000 wydruków
LC6 : KO (czarny i overlay) 600 wydruków
LC8 : YMCKOK 300 wydruków (tylko Tango2e)
Typy kart
PVC ISO CR80. Z paskiem magnetycznym, zbliżeniowe, samoprzylepne oraz karty z HoloPatch
Grubość kart
0,38 mm do 1,6 mm
Pojemność magazynków
Podajnik 100 szt.
Zasobnik kart nadrukowanych 50 szt.
Głowica
300 dpi (wymienna)
Interfejs
Port LPT, USB, Ethernet
Sterowniki
Windows 2000, XP, 2003 Server (user mode)
Zasilanie
90–265 V; 47–63 Hz
Wymiary (szer. x wys. x dł.)
Rio2e – 193,5 mm x 232,5 mm x 369,5 mm
Tango2e – 193,5 mm x 232,5 mm x 471,1 mm
Masa
Rio2e – 7,2 kg
Tango2e – 8,3 kg
Temperatura pracy
10–30°C

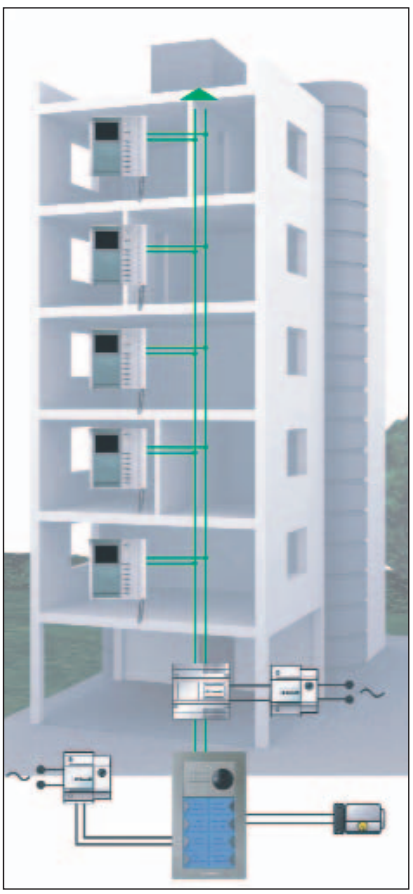
DYSTRYBUTOR w Polsce:

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 022 832 47 44, faks 022 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl

Ultra ELECTRONICS

2-przewodowy, kolorowy system wideodomofonowy

firmy COMELIT



SBC SIMPLEBUS COLOR

Cechy charakterystyczne:

- kolorowe monitory z 4" ekranem LCD
- 2 przewody łącznie z zasilaniem monitora
- 4 magistrale na zasilacz (np. 4 piony w budynku mieszkalnym)
- do 8 monitorów z funkcją intercomu 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
- wyeliminowano konieczność stosowania zasilacza monitora

Oprócz standardowych funkcji systemów wideodomofonowych, monitory Bravo i Genius umożliwiają sterowanie programowalnym modułem przekaźnikowym lub innym zewnętrznym urządzeniem. Standardowo możliwe jest podłączenie przycisku dzwonka lokalnego i dodatkowej (oddalonej) sygnalizacji wywołania. Ponadto monitor Bravo można wyposażyć w kartę 4 dodatkowych przycisków realizujących inne funkcje w systemie (np. przełączanie obrazu z kamer zewnętrznych, interkom itp.)

W systemie Simlpebus2 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. Kamera panelu wejściowego posiada płynną regulację położenia w obu płaszczyznach oraz podświetlanie diodami LED. Ramki zewnętrzne paneli dostępne są w różnych kolorach.

DYSTRYBUTOR w Polsce:

alarmnet®

ALARMNET Sp. j.
ul. Karola Miarki 20C
01-496 Warszawa

tel.: 022 663 40 85
faks 022 833 87 95
www.alarmnet.com.pl

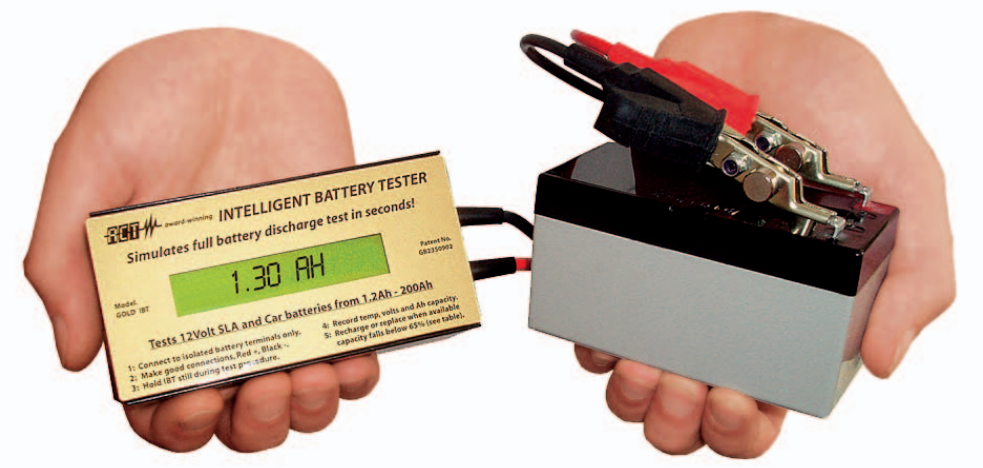
GOLD-IBT

inteligentny tester akumulatorów

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

Jak zmierzyć jego pojemność?

Inteligentny Tester Akumulatorów GOLD-IBT w kilka sekund dokonuje symulacji pełnego rozładowania akumulatora. Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.



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

Dane techniczne:

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

alarmnet®
ALARMNET Sp. j.
ul. Karola Miarki 20C
01-496 Warszawa
tel.: 022 663 40 85
faks 022 833 87 95
www.alarmnet.com.pl

Drukarka HDP5000

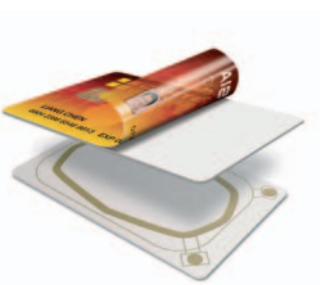
HDP5000 - Specyfikacja Techniczna	
Metoda nadruku:	Retransfer (termodruk retransferowy)
Rozdzielczość:	300 dpi (11.8 punktów/mm)
Kolory:	Do 16,7mln/256 odcieni na piksel
Dostępne rodzaje taśm:	YMC*, pełny kolor, 750 wydruków; YMCK*, pełny kolor z dodatkowym czarnym panelem resinowym, 500 wydruków; YMCKK*, pełny kolor z dwoma czarnymi panelami resinowym, 500 wydruków; YMCKH*, pełny kolor z czarnym panelem resinowym oraz dodatkowym panelem ułatwiającym nadruki na trudnych powierzchniach
Dostępne rodzaje filmu HDP:	– przezroczysty, 1500 wydruków; z hologramem standardowym, 500 wydruków; z hologramem indywidualnym, 500 wydruków.
Dostępne taśmy laminacyjne:	– termotransferowa taśma laminacyjna, przezroczysta, grubość 0,25mil, 500 wydruków; – Folia laminacyjne PolyGuard, grubość 1,0 lub 0,6 mil, 250 wydruków. Wszystkie taśmy laminacyjne dostępne są w opcji: przezroczysta, z hologramem standardowym lub z hologramem indywidualnym.
Prędkość wydruku**:	Przy wydruku seryjnym: 38 sek. na kartę/95 kart na godzinę (YMC*) 46 sek. na kartę/78 kart na godzinę (YMCK*) 70 sek. na kartę/51 kart na godzinę (YMCKK*) 50 sek. na kartę/72 karty na godzinę (YMCK + jednoczesna laminacja dwustronna karty*) 75 sek. na kartę/48 kart na godzinę (YMCKK + jednoczesna laminacja dwustronna karty*)
Rozmiar kart:	CR-80 (85,6 x 54 mm)
Obszar wydruku:	Zadruk całej powierzchni karty, od krawędzi do krawędzi.
Grubość kart:	Tylko druk: 0,762mm – 1,27mm
Druk i laminacja:	0,762mm – 1,02mm
Typ kart:	ABS, PVC, PET, PETG, zbliżeniowe, chipowe, z paskiem magnetycznym,
Pojemność podajnika kart:	100 kart (0,762mm)
Pojemność odbiornika kart:	200 kart (0,762mm)
Czyszczenie kart:	Wymienne rolki czyszczące (w zestawie z każdą taśmą do druku)
Pamięć:	16MB RAM
Wyświetlacz:	SmartScreen, panel kontrolny LCD
Sterowniki:	Windows 2000 / XP / Server2003 / Vista
Opcje kodowania (jeden przewód USB	Kodowanie paska magnetycznego HiCo i LoCo, 1,2,3 ścieżka;
łączy drukarkę i kodery z komputerem)	Procesorowe karty zbliżeniowe (HID iClass i MIFARE); Procesorowe karty stykowe – odczyt i zapis na kartach pamięciowych i mikroprocesorowych zgodnych z ISO7816-1/2/3/4
(T=0, T=1) oraz na kartach synchronicznych;	Czytnik kart HID Prox.
Złącza:	USB 2.0 oraz Ethernet z wewnętrznym serwerem wydruku
Wymagania systemowe:	Procesor x86 lub kompatybilny Windows 200, XP, 2003 lub Vista 500MHz , 256MB RAM min. 500MB wolnej przestrzeni dyskowej
Temperatura pracy:	18-32°C
Wilgotność:	20-80% bez kondensacji
Wymiary (wys/dł/szer) mm:	HDP5000: 292/313/235 HDP5000 + moduł do obracania karty: 292/445/235 HDP5000 + moduł do laminacji jednostronnej: 324/635/235 HDP5000 + moduł do obracania karty + moduł do laminacji dwustronnej: 324/762/235
Moduł laminacyjny:	324/313/235
Waga:	HDP5000: 7,3kg HDP5000 + moduł do obracania karty: 10kg HDP5000 + moduł do laminacji jednostronnej: 12,7kg HDP5000 + moduł do obracania karty + moduł do laminacji dwustronnej: 16,4kg
Normy:	Bezpieczeństwo:UL60950, CSA C2.2 nr 60950, CB (EN 60950), CE EMC: FCC część15 KlasaA, EN55022: 1998 KlasaA, CRC c1374, EN 61000-3-2: 2000, EN61000-3-2: 1995, EN55024: 1998, znak CE oraz CCC
Napięcie:	100-240VAC, 3,8A
Częstotliwość:	50/60kHz
Gwarancja:	Drukarka: 1 rok
Głowica:	gwarancja dożywotnia, bez ograniczeń dotyczących liczby wydruków
Materiały eksploatacyjne Fargo:	Drukarki Fargo wymagają użycia wysokiej jakości materiałów eksploatacyjnych. Aby zmaksymalizować jakość i trwałość nadruku na kartach, żywotność głowicy i niezawodność drukarki należy używać wyłącznie oryginalnych materiałów eksploatacyjnych Fargo. Uzycie nieautoryzowanych przez Fargo materiałów eksploatacyjnych może skutkować utratą gwarancji na urządzenie.
Opcje:	Moduł do laminacji kart – jednostronnie lub dwustronnie (laminacja równoczesna obu stron karty) kodery kart mikroprocesorowych (stykowych i bezstykowych) Zamki do podajników drukarki Zestaw czyszczący do drukarki Koder paska magnetycznego Podajnik na 200 kart Moduł do obracania karty

Drukarka HDP5000 jest najbardziej wszechstronnym urządzeniem do produkcji i kodowania trwałych, wysokiej jakości kart plastikowych.

Karty drukowane na HDP5000 spełniają wysokie wymagania, jakie stawiają:
- agencje i urzędy państwowe;
- duże i średnie korporacje;
- instytucje finansowe;
- uczelnie wyższe.

HDP5000 współpracuje z wieloma typami kart:
- HID iClass
- MIFARE/DESFire
- stykowe karty mikroprocesorowe
- karty zbliżeniowe
- karty z paskiem magnetycznym
- karty Wiegand
- karty z pamięcią optyczną
- karty z kodem kreskowym

Zwiększ wydajność swojego systemu do personalizacji kart – zapraszamy do kontaktu z naszym biurem celem zapoznania się z ofertą na:
- oprogramowanie zabezpieczające i zarządzające pracą drukarek w sieci;
- zabezpieczenia wizualne kart – folie holograficzne uniemożliwiające fałszowanie kart;
- oprogramowanie do projektowania i seryjnego wydruku kart;



* symbole określające typ taśmy, ilość paneli na danej taśmie, gdzie Y=żółty, M=Magenta, C=cyan, K=czarny resinowy.
** współczynnik 'prędkość wydruku' wskazuje przybliżoną prędkość druku i mierzony jest od momentu, kiedy jedna zadrukowana karta wpada do odbiornika do momentu kiedy kolejna karta wpadnie do odbiornika. Współczynnik ten nie uwzględnia czasu kodowania kart ani czasu przetwarzania obrazu przez PC i transferu do drukarki.

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

System wideodomofonowy serii 480

GDE POLSKA wprowadza do sprzedaży nowy system wideodomofonowy przeznaczony do instalacji w biurowcach, budynkach mieszkalnych i osiedlach zamkniętych. System może obsłużyć do 480 abonentów.

System charakteryzuje się bardzo prostą instalacją i programowaniem.

W skład systemu wchodzą:

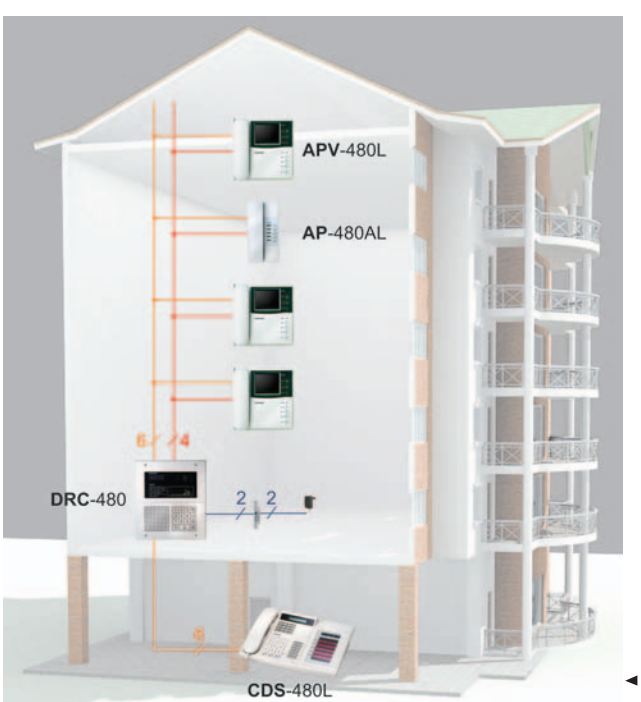
– kamery DRC-480L,
– monitory APV-480L,
– unifony AP-480AL,
– centrale portierskie CDS-480L.

System umożliwia tworzenie zaawansowanych struktur łącząc maksymalnie 99 kamer DRC-480L i 480 monitorów APV-480L. Zamiast monitora (lub równolegle z monitorem) może pracować unifon AP-480AL. Jeśli u jednego lokatora jest zainstalowanych kilka odbiorników (monitorów, unifonów) możliwe jest takie skonfigurowanie systemu aby z kamery wywołać jednocześnie wszystkie odbiorniki lub każdy osobno (kilka kodów użytkowników).

Wywołanie monitorów/unifonów jest możliwe z klawiatury numerycznej na panelu z kamerą. Klawiatura ta umożliwia także otwieranie drzwi wejściowych (system indywidualnych kodów). Opcjonalnie istnieje możliwość otwierania drzwi kartą (czytnik kart zamontowany w kamerze).

Po zainstalowaniu centrali portierskiej mamy możliwość kontroli dostępu osób wchodzących/wychodzących poprzez portiera. Osoba odwiedzająca może nawiązać komunikację bezpośrednio z danym lokatorem wybierając kod abonenta lub (jeśli np. nie znamy kodu abonenta) poprzez portiera, który nawiąże połączenie z danym lokatorem.

W systemie tym jest także możliwość nawiązania rozmowy pomiędzy lokatorami (funkcja interkomu). W tym celu lokator dzwoni do portiera, który nawiązuje połączenie z kolejnym lokatorem.



◄ *Przykładowy schemat podłączenia*

DRC-480L ►

GDE POLSKA
GLOBAL DISTRIBUTOR OF ELECTRONICS

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

tel./fax: 012 256 50 35, 256 50 25
fax: 012 270 56 96
e-mail: biuro@gde.pl

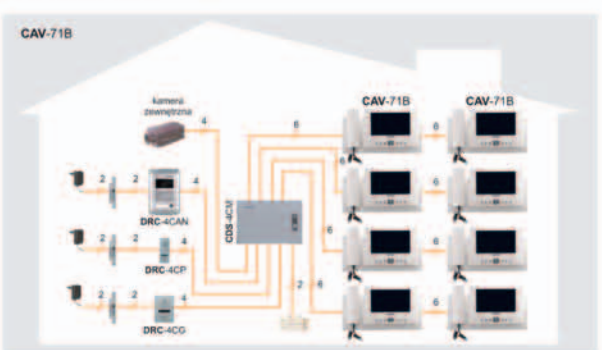
CAV-71B
Monitor kolorowy z łącznością interkomową

CAV-71B to kolorowy monitor w ofercie firmy GDE POLSKA z 7-calowym, panoramicznym wyświetlaczem LCD, na którym oprócz obrazu z kamery wyświetlane są dodatkowe informacje systemowe (data, godzina, menu systemowe, funkcje interkomu).

Elementem łączącym monitory z kamerami jest centrala systemowa CDS-4CM umożliwiająca podłączenie maksymalnie 4 kamer DRC-4C** (obsługa 4 wejść) i 20 monitorów CAV-71B. Centrala CDS-4CM dodatkowo wyposażona jest w moduł pamięci 128 obrazów umożliwiający zapis zdjęć osób odwiedzających np. podczas nieobecności domowników. Zapisane obrazy można przeglądać z dowolnego monitora podłączonego do systemu (1 lub 6 zdjęć jednorazowo wyświetlanych na ekranie).

Ciekawą funkcją monitorów CAV-71B jest interkom pomiędzy użytkownikami systemu. Przy instalacji kilku odbiorników (max. 20) możliwe jest wywołanie z dowolnego monitora CAV-71B każdej innej stacji końcowej (monitora) i rozmowa tylko pomiędzy dwoma użytkownikami końcowymi (selektywne wywołanie interkomowe).

Monitor CAV-71B wyposażony został również w funkcję alarmu. Po uzbrojeniu wejścia kontaktronem (podłączonym do centrali CDS-4CM) i uaktywnieniu funkcji alarmu, w momencie przerwania obwodu zabezpieczeń zostaniemy o tym powiadomieni poprzez generator dźwięku zainstalowany w monitorach.



Okablowanie	Monitor - centrala systemowa: 6 przewodów Centrala systemowa - kamera: 4 przewody
Zasilanie	100-240 V_{AC} 50-60 Hz
Pobór mocy	Czuwanie: 6 W Praca: 19 W
Temperatura pracy	od 0°C do 40°C
Wymiary (szer. x wys. x gł.)	315 mm x 175 mm x 53 mm
Masa	1.7 kg

GDE POLSKA
GLOBAL DISTRIBUTOR OF ELECTRONICS

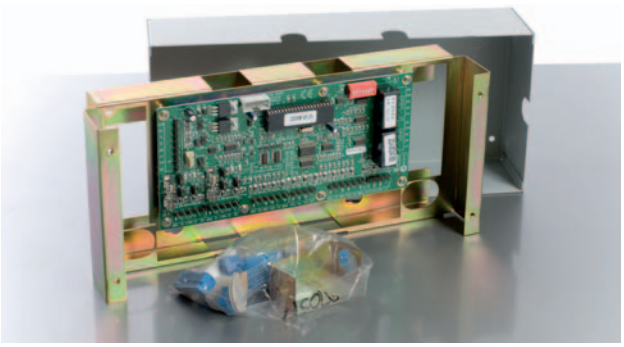
GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

tel./fax: 012 256 50 35, 256 50 25
fax: 012 270 56 96
e-mail: biuro@gde.pl

Moduł kontroli dostępu dla dwóch przejść

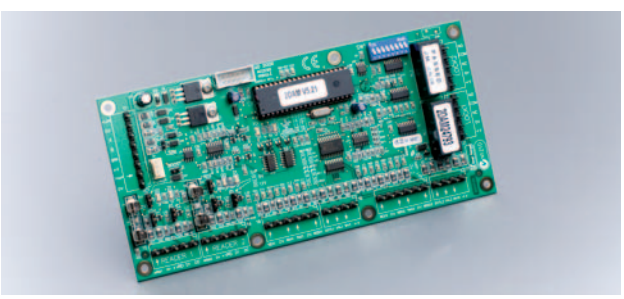
Moduł kontroli dostępu dla 2 przejść służy jako interfejs dla czytników kart systemu kontroli dostępu i systemu alarmowego. System alarmowy w wybranych obszarach może być włączony i wyłączony po wczytaniu ważnej karty. Ponadto, podczas programowania systemu, każdym drzwiom można przyporządkować inny tryb przydziału dostępu (dwóch użytkowników, karta plus kod PIN) oraz funkcję anti-passback. Moduł udostępnia również funkcję DOZD (Drzwi Otwarte Zbyt Długo) oraz wejście linii dozorowej do podłączenia czujnika zaryglowania (Tongue Sesne), a także wyjścia sterujące do sygnalizacji ważnych i nieważnych prób dostępu.

- Moduł współpracuje z popularnymi czytnikami wyposażonymi w interfejs ABA Track II lub Wieganda, bez konieczności stosowania żadnych dodatkowych urządzeń komunikacyjnych.
- Standardowa obsługa w trybie „off-line" maks. 31 kart awaryjnych.
- Wersja z dodatkową pamięcią umożliwia obsługę w trybie „off-line" 35 kart awaryjnych oraz 100 kart dostępu na jedno przejście.
- Monitorowanie rygla i czujnika zaryglowania.
- Wejścia REX (Request to Exit) i REN (Request to Enter) służące do sterowania drzwiami lokalnie lub zdalnie.
- Wyjścia sterujące dla sygnalizacji wejść ważnych i nieważnych oraz drzwi otwartych zbyt długo.
- Przekaźniki sterowania pracą rygli zainstalowane na płycie.
- Bezpiecznik dla złącza magistrali LAN i zasilania zewnętrznego.



995012 Moduł obsługi 2 czytników w obudowie metalowej

995012PS Moduł obsługi 2 czytników z zasilaczem w obudowie metalowej
995012PS Moduł obsługi 2 czytników z i pamięcią off-line, w obudowie metalowej zasilaczem



995012PCB&K Moduł obsługi 2 czytników, płytka PCB
995012CAPCB&K Moduł kontroli dostępu dla 2 przejść z dodatkową pamięcią off-line, płytka PCB

DANE TECHNICZNE	
Parametry fizyczne	
Wymiary obudowy	
995012	305 x 140 x 72 (mm)
995012PS / 995012CAPS	252 x 358 x 85 (mm)
Środowisko pracy	0°C do 40°C przy wilgotności względnej w przedziale 15% do 85% (bez kondensacji pary)
Parametry elektryczne	
Wejście zasilające	11-14 V DC (zwykle podawane z osobnego zewnętrznego układu zasilającego).
Min. prąd pracy	70 mA (bez prądu rygli i urządzeń obciążenia zewnętrznego)
Prąd maksymalny	210 mA
Zabezpieczenie prądowe	500 mA
Wejścia	
Wejścia stref	7 (mogą być predefiniowane)
Porty czytników	2
Wyjścia	
Wyjścia przekaźnikowe	2 (zwykle wykorzystywane dla rygli)
Wyjścia OC	4 (zwykle wykorzystywane dla sygnalizacji wejść ważnych/nieważnych)
Drzwi Otwarte Zbyt Długo	2 (1 na przejście)

ID ELECTRONICS Sp.z o.o.
02-793 Warszawa, ul. Przy Bażantarni 11
tel. 022 649 60 95, faks 022 649 61 00
e-mail: sales@ide.com.pl
www.ide.com.pl

ALARMTECH POLSKA Sp. z o.o.

Detektory wibracji z serii CD 400

Dane techniczne	
Napięcie zasilania	9-15 V DC
Tętnienia maks.	2 Vpp przy 12 V
Pobór prądu w stanie czuwania	9 mA
Pobór prądu w stanie alarmu	11 mA
Rodzaj wyjścia alarmowego	przekaźnik, NC
– rezystancja szeregowa pętli zabezpieczającej	<33 Ohm w szeregu
– obciążalność	100 mA/25 V
– czas podtrzymania alarmu w trybie AUTO	2 s
– sygnalizacja alarmu w trybie MONITOR	dioda LED
Zabezpieczenie niskiego napięcia	<8 V
Zabezpieczenie sabotażowe	mikroprzełącznik, NC, 25 V/100 mA
Ustawienie czułości	potencjometr
Temperatura otoczenia	od -20°C do +50°C
Wilgotność	maks. 90% RH, klasa F
Klasa ochrony obudowy IEC 529	IP 31

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

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

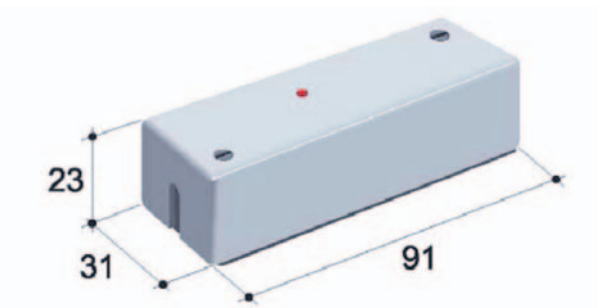
Detektor można montować na elastycznych, wieloelementowych konstrukcjach, takich jak ramy i ościeżnice okien i drzwi, na ceglanych ścianach, gdzie próby ich sforsowania mogą być dokonane z dużą siłą za pomocą tępego narzędzia.

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

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

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

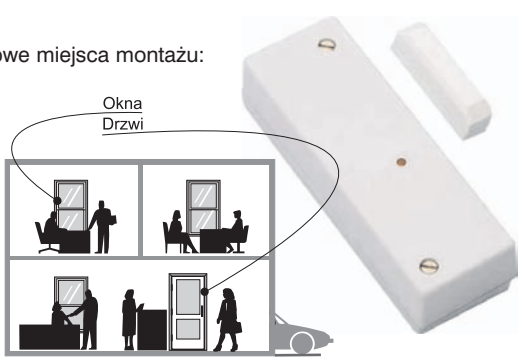
Atest Techom w klasie S.....39/06



Materiał	stal/drewno/szkło	cegła/gips	beton*
Promień detekcji	5 m	2 m	3 m

*) z użyciem płytki montażowej MP 400

Typowe miejsca montażu:



CD 400-R, szczelina 20 mm

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

80-299 Gdańsk-Osowa, ul. Kielnieńska 115
tel. (0-58) 340 24 40, fax (0-58) 340 24 49
http://www.alarmtech.pl, e-mail: info@alarmtech.pl

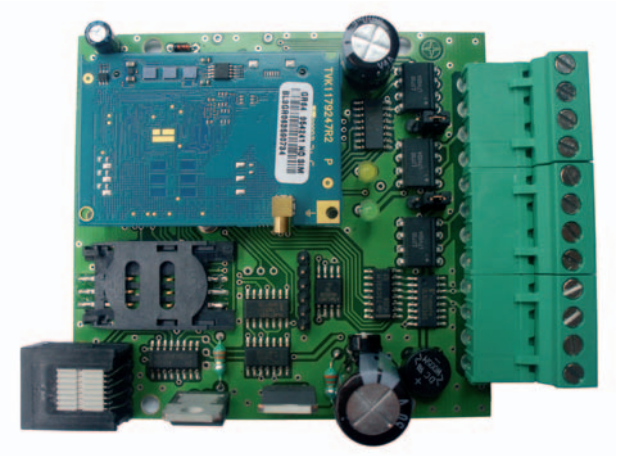
Moduły GSM/GPRS z właściwościami centrali alarmowej

Współpracują również ze wszystkimi typami central alarmowych.

Urządzenia TX400, TX404, TX406 przeznaczone są do monitoringu, komunikacji i powiadamiania o stanach alarmowych chronionych obiektów wykorzystując sieć komórkową dowolnego operatora GSM. Monitoring stanów alarmowych możliwy jest za pomocą zwykłej wiadomości tekstowej SMS lub z wykorzystaniem funkcji Clip do stacji monitoringu.

Urządzenia służą również do zdalnego sterowania innymi urządzeniami wykonawczymi. Każdy z modeli serii TX jest zintegrowany z modułem komunikacyjnym GSM/GPRS i wymaga tylko włożenia aktywnej karty SIM. Poprzez dołączone w zestawie oprogramowanie „TXprog" należy urządzenie odpowiednio zaprogramować i jest ono gotowe do pracy.

Urządzenia przeznaczone są do zastosowań profesjonalnych dla agencji ochrony jak i indywidualnych użytkowników.



Model urządzenia	TX400	TX404	TX406
Wejścia binarne			
Ilość wejść	6	4	6
Optoizolacja wejść	Tak	Tak	Tak
Typ wejść	NO-NC/napięciowe	NO-NC/napięciowe	NO-N /napięciowe
Możliwość blokowania wejść	Tak	Tak	Tak
Reakcje na aktywację wejścia	SMS, Clip zmiana stanu wyjść funkcja blokowania	SMS, Clip zmiana stanu wyjść funkcja blokowania	SMS, Clip zmiana stanu wyjść funkcja blokowania
Reakcje na powrót do stanu normalnego	R	R	R
Wyjścia			
Ilość wyjść	0	2	2
Czasowe przełączanie wyjść	-	Tak	Tak
Wiadomości SMS			
Ilość wiadomości SMS	16	24	24
Formatowanie treści wiadomości SMS	Tak	Tak	Tak
Programator czasowy			
Ilość programowalnych zdarzeń	4	4	4
Rodzaj zdarzeń czasowych	Odstępy czasowe Dokładna godzina	Odstępy czasowe Dokładna godzina	Odstępy czasowe Dokładna godzina
Rodzaj reakcji	R	R	R
Polecenia SMS			
Polecenia standardowe[1]	Tak	Tak	Tak
Max. ilość poleceń użytkownika[2]	brak	8	8
Reakcje na polecenie	R	R	R

R - reakcje takie same jak na aktywacje wejścia binarnego dla danego urządzenia.

[1] Polecenia standardowe - wbudowane polecenia do zdalnej zmiany stanu wyjść, zapytania o stan urządzenia.

[2] Polecenia użytkownika - polecenia o dowolnie konfigurowalnej treści i rodzaju czynności do wykonania przez urządzenie.

inter-Kompas s.c.

inter – Kompas s.c.
33-300 Nowy Sącz
ul. Grottgera 3

tel. (18) 547 40 11
faks (18) 547 40 09
e-mail: interkompas@interkompas.com.pl
www.interkompas.com.pl

Depozytariusze kluczy GE - PROTECTOR

Depozytariusze serii **GE - PROTECTOR** są atrakcyjnymi cenowo, urządzeniami systemu zarządzania kluczy, powstałymi w wyniku współpracy z firmą **GE SECURITY**. Depozytariusz składa się z elektronicznego terminala sterującego drzwiami depozytariusza (opcja: drzwi stalowe z szybą lub pełne), oraz specjalnych metalowych pojemników na klucze.

Terminal umożliwia zarządzanie kluczami i dostępem do depozytariusza, (zarządzanie 2 depozytariuszami do 60 kluczy) dla 1000 użytkowników, - sterowanie - karta, pin kod, pin kod + karta.

Terminal pozwala również na dołączenie do niego każdego rodzaju czytników z protokółem Wiegand i obsługę wielu formatów kart zbliżeniowych. (HID, Mifare, 125 KHz itd.)

Depozytariusz jest rozwiązaniem hybrydowym (elektroniczno- mechanicznym). W rozwiązaniu tym klucze są dodatkowo chronione w specjalnych metalowych pojemnikach zabezpieczonych unikalnym cztero-cyfrowym kodem mechanicznym, dowolnie zmienianym przez użytkownika kluczy. W zależności od potrzeb, pojemniki mogą być różnej wielkości, dopasowane do ilości oraz rozmiaru kluczy.

Cały system może współpracować z kontrolą dostępu i rozliczania czasu pracy. System zawiera oprogramowanie zarządzające, pracujące w sieci LAN/WAN, umożliwiające nadawanie różnego typu uprawnień dla użytkowników (strefy czasowe, tworzenie grup użytkowników itp. oraz tworzenie różnego rodzajów raportów).

Modułowa budowa depozytariusza (w szafach RACK 19”), pozwala na indywidualną konfigurację depozytariusza z dowolną ilością pojemników na klucze.

Depozytariusz stosowany może być w strefach bezpieczeństwa gdzie wymagana jest dodatkowa ochrona klucza, szczególnie dla kluczy do pomieszczeń specjalnych.

Przykładowa konfiguracja depozytariusza

ZALETY:

- Obudowa stalowa z ochroną sabotażową
- Możliwość łączenia depozytariuszy w kaskady
- Różne opcji terminali
- Możliwość współpracy z czytnikiem linii papilarnych
- Możliwość adaptacji do różnych systemów kontroli dostępu
- Praca samodzielna lub w magistrali RS 485 i LAN
- Oryginalne lub adaptowane do potrzeb użytkownika oprogramowanie
- Pełna ochrona pojemników na klucze
- Prosty montaż i obsługa
- Dostęp tylko do wybranych kluczy w zależności od uprawnień
- Identyfikacja miejsca przechowywania klucza w pojemniku za pomocą diody LED
- Współpraca z systemem CCTV - sterowanie DVR
- Zasilanie: 12VDC, max 1A, akumulator
- Montaż: uchwyty typu RACK
- Modułowa budowa

PROTECTOR

Protector Polska Sp. z o.o.
ul. Tyniecka 28
71-019 Szczecin

tel. 091 431 83 10, faks 091 431 83 11
e-mail: biuro@protector-polska.pl
http://www.protector-polska.pl

Kamera
SAMSUNG SPD - 1000 P

TRYB	SPD - 1000 P
Zasilanie	12V DC (± 10%)
Pobór mocy	Max 6W
Przetwornik obrazu	1/4" CCD
Całkowita ilość pixeli	795 (H) x 596 (V)
Efektywna ilość pixeli	752 (H) x 582 (V)
Synchronizacja	Wewnętrzna
Częstotliwość skanowania	15.625 kHz (H)/50.00 Hz (V)
Rozdzielczość	Kolor: 520TVL (Min.)/B/W: 570TVL (Min.)
Wyjście wideo	1.0 V p-p /75 ø
Stosunek sygnał/szum	50dB (AGC wył.)
Minimalne oświetlenie	0,7 Lux@F1.8 (tryb kolor) 0,02 Lux@F1.8 (tryb B/W) 0,005 Lux@F1.8 (tryb sens-up)
Funkcja Dzień/Noc	Auto/Kolor/B/W (filtr IRC)
Prędkość elektronicznej migawki	Auto/Ręczne (1/50~ 1/120,000 sek.)
Migawka	Włączona (2X ~128X)/Wyłączona
Balans bieli	ATW/AWC/Ręczne (1800°K ~ 10,500°K)
Regulacja wzmocnienia	Auto/Ręczna
OSD	Włączone/Wyłączone (Angielski, Chiński, Francuski, Niemiecki, Hiszpański, Włoski)
Cyfrowy ZOOM	2X ~ 10X (Max. 100X zoom)
Zakres ogniskowej	f 3.8 ~ 38mm (10X)
Sterowanie	PELCO-D, SEC, Panasonic, Vicon, Honeywell etc.
Komunikacja	RS - 485
Minimalny dystans od obiektu	1,5m
Prędkość ZOOM-u	1,75 s
Kąt obrotu w poziomie	350°
Szybkość obrotu w poziomie	140°/s (64 poziomy)
Kąt obrotu w pionie	5° do 185°
Szybkość obrotu w pionie	100°/s (64 poziomy)
Strefy prywatności	Włączone/Wyłączone (4 programowalne strefy)
Programowane pozycje	max 128
Cyfrowy obrót (flip)	Włączony/Wyłączony
Temperatura robocza	(-10°C ~ + 50°C)
Wilgotność	20% ~ 75% bez kondensacji
Wymiary	Ø 140(W) x 134.8(H) mm
Masa	0.8 kg

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: cctv@ccpartners.pl
www.samsungcctv.ccpartners.pl

CZASOPISMO
ZABEZPIECZENIA
ul. Puławska 359, 02-801 Warszawa
tel. 022 546 09 51, faks 022 546 09 59

....., dn. ..... 2008 r.

ZAMÓWIENIE

NA WPIS DO SPISU TELEADRESOWEGO

Zamawiamy ogłoszenie reklamowe w spisie teleadresowym „Zabezpieczeń":

☐ 6 emisji = 360 zł + VAT ☐ 12 emisji = 648 zł + VAT

Nr i rok wydania: ...../.....

OŚWIADCZENIE

Oświadczamy, że firma .....
jest płatnikiem uprawnionym do otrzymywania faktur VAT zgodnie z Rozporządzeniem Ministra Finansów z dnia 18 kwietnia 1995 r. w sprawie podatku od towarów i usług (Dz. Ust. Nr 41, poz. 212 z późniejszymi zmianami).

Upoważniam firmę:
AAT Trading Company Spółka z o.o., ul. Puławska 431, 02 - 801 Warszawa,
Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy KRS, KRS 0000058658, NIP: 951-10-01-169
wysokość kapitału zakładowego 5600000,00 zł, nr rej. GIOŚ: E0001894W,
wydawcę czasopisma „Zabezpieczenia" do wystawiania faktur VAT bez podpisu odbiorcy.

Forma płatności: przelew

DANE NA FAKTURZE:

Nazwa firmy: .....

.....

Adres (ulica, nr domu) .....

.....

(kod, miejscowość) .....

.....

NIP: .....

Imię i nazwisko oraz nr telefonu osoby, z którą można uzgadniać szczegóły techniczne reklamy:

.....

.....

AKTUALNE DANE TELEADRESOWE:

Nazwa firmy: .....

.....

Adres (ulica, nr domu) .....

.....

(kod, miejscowość) .....

.....

Telefon: .....

.....

Faks: .....

E-Mail: .....

www: .....

KATEGORIE

- ☐ Systemy sygnalizacji włamania i napadu
- ☐ Systemy telewizji dozorowej
- ☐ Systemy kontroli dostępu
- ☐ Systemy sygnalizacji pożarowej
- ☐ Systemy ochrony peryferyjnej
- ☐ Integracja systemów
- ☐ Monitoring
- ☐ Zabezpieczenia mechaniczne
- ☐ Systemy nagłośnień

DZIAŁALNOŚĆ

- ☐ Produkcja
- ☐ Projektowanie
- ☐ Dystrybucja
- ☐ Instalacja
- ☐ Szkolenia

Imię i nazwisko osoby zamawiającej:

.....

.....

podpis, data i pieczęć firmy

Prosimy także o przesłanie na nośniku elektronicznym bądź e-mailem zabez@zabezpieczenia.com.pl loga Państwa firmy w CMYK-u w formacie eps, cdr, ai, tif lub jpg.

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 27A
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. Racławicka 82, 60-302 **Poznań**
tel. (61) 662 06 60
faks (61) 662 06 61

ul. Mieszczańska 18, 30-313 **Kraków**
tel. (12) 266 87 95
tel./faks (12) 266 87 97

Al. Niepodległości 659, 81-855 **Sopot**
tel. (58) 551 22 63
tel./faks (58) 551 67 52

ul. Zielona 42, 71-013 **Szczecin**
tel. (91) 483 38 59, 489 47 23
faks (91) 489 47 24

ul. Na Niskich Łąkach 26, 50-422 **Wrocław**
tel./faks (71) 348 20 61
tel./faks (71) 348 42 36

ul. Ks. W. Siwka 17, 40-318 **Katowice**
tel. (32) 351 48 30
tel. (32) 256 69 34
tel./faks (32) 256 60 34

ul. Dowborczyków 25, 90-019 **Łódź**
tel./faks (42) 674 25 45
tel./faks (42) 674 25 48

ul. Łęczycka 37, 85-737 **Bydgoszcz**
tel./faks (52) 342 91 24, 342 98 82

ACIE Polska Sp. z o.o.
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. Portowa 14, 44-100 **Gliwice**
tel. (32) 790 76 23
faks (32) 790 76 65
e-mail: gliwice@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. Pachońskiego 2a, 31-223 **Kraków**
tel. (32) 790 76 46
faks (32) 790 76 73
e-mail: krakow@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. (71) 363 38 93
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.
Security Systems
ul. Poleczki 3
02-822 Warszawa
tel. (22) 715 41 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

C&C PARTNERS TELECOM Sp. z o.o.
WYŁĄCZNY AUTORYZOWANY DYSTRYBUTOR SAMSUNG TECHWIN W POLSCE
ul. 17 Stycznia 119,121
64-100 Leszno
tel. (65) 525 55 55
faks (65) 525 56 66
e-mail: cctv@ccpartners.pl
www.samsungcctv.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. Morcinka 5 paw. 6
01-496 Warszawa
tel. (22) 638 44 40
faks (22) 638 45 41
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 Sp. z o.o.
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 08 88
faks (22) 546 06 19
e-mail: mail@cma.com.pl
www.cma.com.pl

Oddział:
ul. Świętochłowicka 3, 41-909 **Bytom**
tel. (32) 388 09 50
faks (32) 388 09 60

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+H Polska Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
Dział SAP: tel. (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. Kielnieńska 134A, 80-299 **Gdańsk**
tel. (58) 554 47 46
faks (58) 552 45 24

ul. Płochocińska 19 lok. 43, 03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

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

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
ul. Ciepła 15/50
50-524 Wrocław
tel. (71) 367 06 16, 364 78 64
faks (71) 367 06 16
e-mail: biuro@delta-dbs.pl
www.delta-dbs.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
www.ebs.pl

EDP Support Polska Sp. z o.o.
ul. Chłapowskiego 33
02-787 Warszawa
tel. (22) 644 53 90, 644 51 53
faks (22) 644 35 66
e-mail: edps@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, 42 30 728
faks (32) 42 30 729
e-mail: el-mont@el-mont.com
el-mont@internetdsl.pl
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 01-03
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. 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

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

GE Security Polska Sp. z o.o.
ul. Sadowa 8
80-771 Gdańsk
tel. (58) 301 38 31, 760 64 80
faks (58) 301 14 36
www.gesecurity.pl

Oddziały:
Al. Stanów Zjednoczonych 59
04-028 **Warszawa**
tel. (22) 810 00 03
faks (22) 810 10 55

Os. Na Murawie 11/2, 61-655 **Poznań**
tel. (61) 821 35 66
faks (61) 821 31 94

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.com

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. +48 693 029 278
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. 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. 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. 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
faks (58) 341 44 90
e-mail: info@kolektor.com.pl
www.kolektor.com.pl

KOLEKTOR
K. Mikiciuk, R. Rutkowski Sp. J.
ul. Krzywoustego 16
80-360 Gdańsk-Oliwa
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

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. Serocka 10, 04-333 **Warszawa**
tel. (22) 610 40 13
faks (22) 610 37 28

infolinia: 0 801 055 075

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
fax, (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

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, 363 92 60
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV
ul. Heleny Szafran 10
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
fax (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, www.zasilacze.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./faks (22) 676 77 37
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
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

SAMAX S.A.
ul. Mińska 25
03-808 Warszawa
tel./faks (22) 813 44 25, 870 43 80, 870 77 36
e-mail: samax@samax.pl
www.samax.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 5
02-675 Warszawa
tel. (22) 60 60 614÷617
faks (22) 60 60 618
e-mail: office.warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddział:
ul. M. Palacza 13
60-242 **Poznań**
tel. (61) 66 43 140 - 42
faks +48 61 66 43 143
e-mail: office.poznan@schrack-seconet.pl

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

Security System Integration S.A.
ul. Irysowa 4
Bielany Wrocławskie
55-040 Kobierzyce
tel. (71) 33 07 900, 33 07 901
faks (71) 33 07 906
e-mail: ssi@ssisa.pl
www.ssisa.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

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

OLAR ELEKTRO Sp. z o.o.
ul. Rokicińska 162
92-412 Łódź
tel. (42) 677 58 00
faks (42) 677 58 01
e-mail: communication@solar.pl,
security@solar.pl
www.solar.pl

Oddziały:
ul. Łużycka 3B
81-537 **Gdynia**
tel. (58) 662 00 00/04/05
tel. 0 603 963 695
faks (58) 664 04 00

ul. Radzikowskiego 35
31-315 **Kraków**
tel. (12) 638 91 16
tel. 0 605 366 396
faks (12) 638 91 22

ul. Witosa 3
20-330 **Lublin**
tel. (81) 745 59 00
faks (81) 745 59 05

ul. Smoluchowskiego 7
60-179 **Poznań**
tel. (61) 863 02 04
faks (61) 863 02 70

ul. Heyki 3
70-631 **Szczecin**
tel. (91) 485 44 00
tel. 0 601 570 247
faks (91) 485 44 01

ul. Krakowska 141-155
50-428 **Wrocław**
tel. (71) 377 19 12
tel. 0 607 038 023
faks (71) 377 19 19

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) 431 00 04
faks (91) 462 48 95
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

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

www.aper.com.pl
www.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 SECURITY
ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.s7.pl, www.sevenguard.com,
www.system7.biz

TAP Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. (61) 876 70 88
faks (61) 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. (22) 843 83 95
faks (22) 843 79 12
e-mail: tap5@tap.com.pl

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

A DIVISION OF CCTV SYSTEM 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
faks (22) 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

TP TELTECH

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60, 639 88 72
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
ul. Długa 22/27
80-801 **Gdańsk**
tel. (58) 302 52 12
faks (58) 346 25 09
e-mail: michal.mikolajski@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. Rakowiecka 51
31-510 **Kraków**
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Rzeczypospolitej 5
59-220 **Legnica**
tel./faks (76) 856 60 71
e-mail: marian.sitko@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 8 445
faks (22) 430 8 302
gsm +48 600 880 798
e-mail: tokon@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 do 10
faks (61) 872 96 30

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

WIZJA

WIZJA Sp. z o.o.
ul. Zakładowa 6
62-052 Komorniki k. Poznania
tel. (61) 810 08 00
faks (61) 810 08 10
www.wizja.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	-
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	-
COM-LM	TAK	TAK	TAK	TAK	-
CONTROL SYSTEM FMN	-	TAK	TAK	TAK	TAK
D+H Polska	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	TAK	-	TAK
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compil	TAK	TAK	TAK	-	TAK
El-Mont	TAK	TAK	-	TAK	-
Elproma	-	TAK	-	TAK	-
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy-Instalacje	-	TAK	-	TAK	TAK
Emu	-	-	TAK	-	-
Eureka	-	TAK	-	TAK	-
FES	-	TAK	TAK	TAK	-
GE Security Polska	-	-	TAK	-	TAK
Gunnebo	TAK	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
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	-	-	-	-
Miwi-Urmet	TAK	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	-	-	-	-
Sagitta Sp. z o.o.	TAK	-	-	-	-
Samax	TAK	TAK	-	TAK	TAK
Satel	TAK	TAK	-	-	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	-	-
Sprint Sp. z o.o.	-	TAK	-	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	-	TAK
SSI	TAK	TAK	-	TAK	-
STRATUS	-	TAK	TAK	-	TAK
SYSTEM 7 SECURITY	TAK	TAK	TAK	-	TAK
TAC	-	TAK	TAK	TAK	-
Talcomp	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	-	-	TAK	-	TAK
Tayama	TAK	TAK	TAK	TAK	TAK
Techom	-	-	-	-	TAK
Technokabel	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	-	-
Wizja	-	-	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	-	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
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	-	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	-	-
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
CONTROL SYSTEM FMN	TAK	TAK	TAK	-	-	TAK	-	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	TAK
ela-compil	-	-	-	-	-	TAK	-	-	-
El-Mont	TAK	TAK	TAK	-	TAK	-	-	-	-
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	-	-	-
Elza Elektrosystemy-Instalacje	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
EMU	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	-	TAK	TAK	TAK	-	-
FES	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
GE Security Polska	TAK	TAK	TAK	TAK	TAK	TAK	-	-	-
Gunnebo	-	-	TAK	-	-	-	-	TAK	-
GV Polska	-	TAK	-	-	-	-	TAK	-	-
HSA	TAK	TAK	TAK	TAK	TAK	-	-	-	-
ICS Polska	TAK	TAK	TAK	-	-	-	-	-	-
ID Electronics	TAK	TAK	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	-
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
MicroMade	-	-	TAK	-	Rejestracja czasu pracy			-	-
Miwi-Urmet	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	-	-	-	-	-	-
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	TAK	-
PPH Pulson	-	-	-	-	-	TAK	TAK	-	-
Radioton	-	TAK	-	-	-	-	-	-	-
Ramar	TAK	TAK	TAK	-	TAK	-	TAK	-	-
ROPAM Elektronik	TAK	-	-	TAK	-	-	TAK	-	-
Sagitta Sp. z o.o.	-	-	-	TAK	-	-	-	-	-
Samax	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Satel	TAK	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
Sprint Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
SSI	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
SYSTEM 7 SECURITY	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	-	TAK	-	-	-	-
Tayama	TAK	TAK	TAK	-	-	TAK	-	-	TAK
Techom	TAK	-	-	-	-	-	-	-	-
Technokabel	wszystkie rodzaje kabli								
TP TELTECH	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Trikon	-	-	TAK	-	-	-	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
UNICARD S.A.	-	-	TAK	-	-	TAK	-	TAK	-
W2	TAK	-	-	TAK	-	-	-	-	-
Wizja	-	-	-	-	-	-	-	-	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 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
rafał@zabezpieczenia.com.pl
Andrzej Sosiński
andrzej@zabezpieczenia.com.pl
Współpraca
Jarosław Barszcz
Sławomir Wagner
Marcin Pyclik
Dział DTP
PLUPART
01-682 Warszawa,
ul. Kiwerska 34 lok 1
tel: (022) 833 72 22. 833 14 14
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 46
faks (22) 546 05 01
Druk
Heldruk
ul. Partyzantów 3b, Malbork

Cennik reklam

cała strona, pełny kolor	– 3600 zł
cała strona, czarno–biała	– 2100 zł
1/2 strony, pełny kolor	– 2200 zł
1/2 strony, czarno–biała	– 1300 zł
1/3 strony, pełny kolor	– 1700 zł
1/3 strony, czarno–biała	– 1000 zł
1/4 strony, pełny kolor	– 1300 zł
1/4 strony, czarno–biała	– 800 zł
karta katalogowa, 1 strona	– 800 zł
artykuł sponsorowany	– indywidualne negocjacje

Reklama na okładkach

pierwsza strona	– indywidualne negocjacje
druga strona	– 5000 zł
przedostatnia strona	– 5000 zł
ostatnia strona	– 5000 zł

Spis teleadresowy

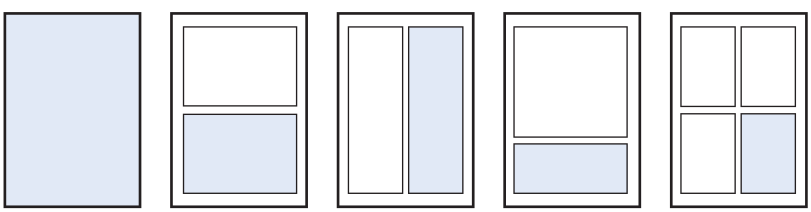
jednorazowy wpis	– 60 zł

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji.

W przypadku zamówienia na 12 emisji – 10% rabat.

Podane ceny nie uwzględniają podatku VAT (22%).

Nr konta: **AAT Trading Company Sp. z o.o.**
PKO SA VIII Oddział/Warszawa 34124011121111000001649659



cała strona	1/2 strony	1/2 strony	1/3 strony	1/4 strony
199,5 x 282,15 mm + 3 mm spad	170 x 125 mm	81,5 x 257 mm	170 x 80,5 mm	81,5 x 125 mm

Materiały reklamowe przyjmowane są tylko w formie elektronicznej.

Redakcja przyjmuje pliki w CMYK-u w plikach:

- **tiff** – 1 warstwa, rozdzielczość 300 dpi,
- **eps, ai, pdf** – teksty zamienione na krzywe, rozdzielczość bitmap 300 dpi, PDF 1.3,
- **cdr** – do wersji 11, teksty zamienione na krzywe, rozdzielczość bitmap 300 dpi,
- **jpg** – możliwie najwyższa jakość (*maximum quality*), rozdzielczość 300 dpi.

Uwaga!

Reklamy całostronicowe muszą zawierać min. 3 mm spady z każdej strony.

Redakcja nie ponosi odpowiedzialności za zgodność kolorów w innej niż CMYK przestrzeni kolorystycznej.

Redakcja przyjmuje materiały reklamowe na płytach CD lub e-mailem (do 5 MB).

Materiały należy dostarczyć na 3 tygodnie przed planowanym zamknięciem numeru.

SPIS REKLAM

Międzynarodowe Targi Poznańskie

securex 2008 POLAND

Targi z rekomendacją Polskiej Izby Przemysłu Targowego

Największa Międzynarodowa Wystawa Zabezpieczeń

22-25.04.2008 Poznań

Zapraszamy na największe targi branży zabezpieczeń w Polsce!
Zabezpiecz swój sukces!

Już teraz zaplanuj swój udział na targach SECUREX 2008

Najnowsze systemy zabezpieczeń
Nowe możliwości współpracy
Bezpośrednie kontakty

BEZPIECZEŃSTWO — OCHRONA — MONITORING

Siła SECUREXU to prezentowana przez Państwa bogata oferta oraz profesjonalni Zwiedzający, z których*:

- 78,7 % przyjeżdża by poznać nowości branży
- 89,7% jest zadowolonych z wizyty na targach
- 97,1% deklaruje swój udział w kolejnej edycji targów
- 88,2% uważa targi za pomocne przy podejmowaniu decyzji handlowych
- 91,2% sądzi, że targi to użyteczne narzędzie marketingowe

*na podstawie badania marketingowego przeprowadzonego wśród zwiedzających targów SECUREX 2006

Międzynarodowe Targi Poznańskie sp. z o.o.
ul. Głogowska 14, 60-734 Poznań, e-mail: securex@mtp.pl
Tel. 061 869 25 75, 061 869 22 02, Fax 061 866 29 99

www.securex.pl

Jesteśmy członkiem: ufi CENTREX

Nowe czytniki iCLASS:

Cena ▶ taka sama jak Prox

Montaż ▶ taki sam jak Prox

Pobór mocy ▶ taki sam jak Prox

Bezpieczeństwo ▶ takie jak w Alcatraz

hidcorp.com

Czytniki iCLASS oferują zwiększony poziom bezpieczeństwa z zachowaniem wszystkich funkcji technologii zbliżeniowej. Nowe czytniki iCLASS posiadają identyczne parametry czytników Prox, dotyczące poboru mocy, łatwości instalacji i użytkowania oraz ceny. Jedyną znaczącą różnicą jest zwiększone bezpieczeństwo uzyskane dzięki kodowaniu i wspólnej identyfikacji kart. Możliwość odczytu/zapisu umożliwia wykorzystanie dodatkowych funkcji takich jak biometria, rejestracja czasu pracy, bezpieczne logowanie do komputerów i wiele innych. Ponadto, technologia iCLASS jest dostarczana przez HID. Dlatego też, możecie się czuć bezpiecznie.

HID

ACCESS security.

iCLASS