CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 4(56)/2007

ZABEZPIECZENIA

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

z nami bezpieczniej

W NUMERZE:

- Mechanizmy zabezpieczeń w sieciach WiMAX
- Przegląd czujek wielodetektorowych Polon-Alfa
- EIB – rozproszony system zarządzania budynkiem (część 2.)
- Zagrożenie podsłuchem bezprzewodowych radiowych klawiatur komputerów

urmet
MIWI

iProtect™

ZINTEGROWANY SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM

Kontrola Dostępu

Rejestracja Czasu Pracy

CCTV IP

SSWiN

Parking

Ochrona Osób

Integracja z systemem PPOŻ

Rejestracja Gości

TCP/IP

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

CZASOPISMO ZABEZPIECZENIA 4/2007

w numerze

WYDARZENIA INFORMACJE 4

SYSTEMY ZINTEGROWANE

EIB – rozproszony system zarządzania budynkiem (cz. 2)
– *Jerzy Mikulik, AGH* 28

OCHRONA PRZECIWPOŻAROWA

Przegląd czujek wielodetektorowych Polon-Alfa
– *Lech Światły* 33

OCHRONA INFORMACJI

Zagrożenie podsłuchem bezprzewodowych radiowych klawiatur komputerów
– *Adam E. Patkowski, Robert Piotrowski*. 36

Teoria ochrony informacji (część 2.)
– *Marek Blim* 42

Mechanizmy zabezpieczeń w sieciach WiMAX
– *Krzysztof Cabaj, Wojciech Mazurczyk, Krzysztof Szczypiorski*. 54

TELEWIZJA DOZOROWA

Kamery szybkoobrotowe CAMA-I
– *Patryk Gańko, Novus* 60

SYSTEMY KOMUNIKACJI GŁOSOWEJ

Przemysłowy system komunikacji wewnętrznej
– *Przemysław Kaźmierczak, C&C Partners Telecom*. 64

SSWiN

Analiza niezawodnościowa złożonego systemu bezpieczeństwa dla obiektu o specjalnym przeznaczeniu,
– *Waldemar Szulc, Adam Rosiński, Politechnika Warszawska* 67

Czujki CX-502, CX-502AM, CX502AMplus
– *Jarosław Gibas, Optex Security* 74

Transmisja w centralach serii Comfort. Moduł GSM/GPRS CS7002
– *Witold Bach, GE Security* 77

MONITORING

Transmisja bezprzewodowa obrazu i dźwięku 5,8 GHz
– *Jowita Kuczyniecka, „3D" Bydgoszcz* 79

Nowa stacja odbiorcza monitorowania systemów alarmowych z wykorzystaniem sieci GSM/GPRS
– *Dariusz Janusek, Rafał Miklaszewski, Pulson* 81

KONTROLA DOSTĘPU

Drukarka Tango +L
– ACSS 85

KARTY KATALOGOWE 87

SPIS TELEADRESOWY 96

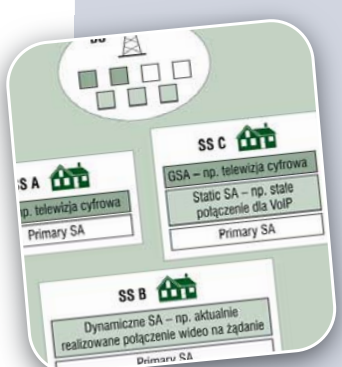
CENNIK REKLAM 106

SPIS REKLAM 106

28
EIB – rozproszony system zarządzania budynkiem

33
Przegląd czujek wielodetektorowych

36
Zagrożenie podsłuchem bezprzewodowych radiowych klawiatur komputerów



54
Mechanizmy zabezpieczeń w sieciach WiMAX

Ponownie w elitarnym klubie *Gazel Biznesu*

Z prawdziwą przyjemnością informujemy, iż po raz kolejny **AAT Trading Company** została uhonorowana prestiżowym wyróżnieniem w rankingu **Gazele Biznesu 2006**, organizowanym przez PULS BIZNESU i międzynarodową wywiadownię gospodarczą Coface Intercredit Poland. Rokrocznie kryteria doboru firm do rankingu są takie same. Podstawowe znaczenie ma więc szybki i stały rozwój w kolejnych trzech latach, wiarygodność biznesowa oraz stabilność na rynku.

Zaliczenie AAT Trading Company po raz drugi z rzędu do grona elitarnego klubu Gazel Biznesu, nie tylko potwierdza jej wysoką pozycję w sektorze małych i średnich przedsiębiorstw, ale i w sposób szczególny motywuje do dalszego, dynamicznego rozwoju jako rzetelnego partnera biznesowego.

Osiągnęliśmy wspólny sukces, za który chcemy Wszystkim Państwu serdecznie podziękować!

AAT Trading Company

18-21 września 2007, Düsseldorf

Targi A+A 2007
– zapowiedź

W dniach 18–21 września 2007 w Düsseldorfie już po raz 27. odbędą się A+A Międzynarodowe Targi Ochrony Osobistej, Bezpieczeństwa i Higieny Pracy.

Poprzednią edycję targów w roku 2005 (targi organizowane są co dwa lata) odwiedziło 54 438 gości, w tym ponad 10 000 z zagranicy. Obejrzeli oni ekspozycje 1370 wystawców z 55 krajów.

A+A oferuje ekspertom z kraju i z zagranicy unikatowe połączenie **targów**, **kongresu** i **wystaw specjalnych**.

W tym roku na tematykę **targów** składają się trzy główne zagadnienia:

- **ochrona osobista** – środki ochrony osobistej, modne stroje robocze oraz bezpieczne maszyny i urządzenia,
- **zdrowie w miejscu pracy** – medycyna pracy, środowiska oraz podróży, prewencja, wyposażenie stanowiska pracy (ergonomia),
- **bezpieczeństwo korporacyjne** – m.in. ochrona przeciwpożarowa, ochrona środowiska oraz urządzenia pomiarowo-kontrolne.

W halach targowych w Düsseldorfie prezentowane będą produkty i usługi istotne dla ochrony osobistej oraz bezpieczeństwa i higieny pracy.

Targom, tradycyjnie już, towarzyszy 30. **kongres A+A** (około 6 000 uczestników w 2005 roku). Dyskusje będą się toczyły wokół takich tematów jak reformy bezpieczeństwa przemysłowego, wprowadzanie narodowych standardów itp. Znaczenie kongresu wzmocnią międzynarodowe eventy dotyczące m.in. narodowych strategii poprawy warunków pracy organizowane przez International Labour Organization (ILO) oraz the European Agency for Safety and Health at Work (OSHA).

Tematyka kongresu A+A obejmuje sprawy ekonomiczne, tematy zdrowotne (np. choroby zawodowe), możliwości kształtowania miejsca pracy z uwzględnieniem wymogów wynikających ze specyficznych ryzyk i zagrożeń (postępowanie z substancjami niebezpiecznymi) aż po aspekty techniczne (np. bezpieczne urządzenia, środków ochrony osobistej itp.).

Tematy stale zyskujące na znaczeniu to prewencyjna ochrona przeciwpożarowa oraz ergonomia stanowiska pracy. Aspekt ergonomiczny obejmuje wszystkie czynniki przyczyniające się do zapewnienia wydajności pracy.

Trzecim istotnym punktem imprezy będzie specjalna **wystawa** zorganizowana przez wystawców z sektora non-profit „Safety + Health Meeting Place" (Bezpieczeństwo i zdrowie) oraz fora „Good Practice" (Dobre praktyki) i „Science and Research" (Nauka i badania).

Najbardziej aktualne informacje o przygotowaniach do imprezy można znaleźć na stronie internetowej A+A:

http://www.AplusA-online.de

lub na stronie biura polskiego przedstawicielstwa targów:

http://www.as-mwsse.pl

Adres mailowy biura:

biuro@as-messe.pl.

Zapraszamy do udziału w targach.

Redakcja

Nazwa wystawy	A+A 2007 Ochrona osobista, bezpieczeństwo i higiena pracy w zakładach
Miejsce wystawy	Düsseldorf, tereny targowe – hale 1-7.2, teren otwarty i Congress Center Düsseldorf
Terminarz	Dni targowe: 18.09.-21.09.2007 Godziny otwarcia: 9.00-18.00
Karty wstępu	W sklepie online (od sierpnia 2007): • bilet dzienny: 20 euro • bilet dzienny dla uczniów i studentów: 13 euro Bezpośrednio w kasie: • bilet dzienny - 25 euro • bilet dzienny dla uczniów i studentów: 13 euro

Forum Monitoringu Polskiego

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **„Polalarm"** zaprasza do udziału w **X Forum Monitoringu Polskiego**. Forum odbędzie się w dniach **10–11 października 2007 roku** w Centrum Szkoleń i Konferencji GEOVITA w Jadwisinie (ul. Ogrodowa 31, Serock).

Do udziału w seminarium zapraszamy przedstawicieli producentów, dystrybutorów, instalatorów oraz użytkowników monitoringu ze wszystkich dziedzin gospodarki, zainteresowanych rozwojem monitoringu w Polsce.

Program forum obejmuje trzy panele tematyczne, kończące się dyskusją.

Panel 1. Nowe podejście do monitoringu. Zagadnienia prawno-organizacyjne wpływające na efektywność biznesową SMA (systemów monitorowania alarmów)

1. Nowe trendy w monitoringu. Perspektywy rozszerzenia monitoringu wizyjnego na inne branże produkcyjne, usługowe oraz eksploatacyjne – przykłady branż i dziedzin, punkt widzenia osób i firm korzystających z nowych form monitoringu – inż. Bogdan Tatarowski.
2. Weryfikacja sygnałów alarmowych przez operatorów SMA w celu ograniczenia liczby wyjazdów grup interwencyjnych na fałszywe alarmy. Nowe trendy obsługi klientów korporacyjnych – mgr inż. Krzysztof Ciesielski.
3. Elementy zarządzania nowoczesną stacją monitorowania – mgr inż. Krzysztof Ciesielski.
4. Nowe kierunki jakościowe w Normach Europejskich dotyczących monitoringu oraz wykorzystanie ich pod kątem obsługi klientów europejskich i anglojęzycznych na terenie Polski (metoda przejścia z PN na PN-EN) – mgr inż. Andrzej Starnawski.
5. Warunki i możliwości ubezpieczenia działalności związanej z zabezpieczeniami technicznymi (w tym monitoringu). Zakres wyposażenia polisy, czynniki wpływające na wysokość składki – mgr Katarzyna Szczepańska, General Brokers.
6. Aktualne wymagania policji dotyczące zabezpieczenia stacji monitorowania alarmów. Wyposażenie operatorów stacji monitorowania w broń palną, z uwzględnieniem planu ochrony. Zatwierdzenie planów ochrony dla SMA w komendach wojewódzkich Policji. Oczekiwania klientów związane z synchronizacją planów ochrony monitorowanych obiektów z planem ochrony SMA – mgr inż. Lech Wicherkiewicz.

Panel 2. Zagadnienia techniczne w monitoringu alarmowym obiektów stacjonarnych i ruchomych

7. Przykłady nowych zastosowań i rozwiązań techniczno-funkcjonalnych w monitoringu opartym na pakietowej transmisji danych w sieciach GSM – urządzenia serii PX i EX z DTMF. Prezentacja nowego polskiego urządzenia i systemu kontroli służb dozoru wartowników i ochrony fizycznej Active Guard – mgr inż. Witold Górzyński, TASC Technology, mgr inż. Adam Paulski, EBS.
8. Wykorzystanie sieci IP do przesyłu informacji związanych z monitoringiem alarmowym oraz monitoringiem wizyjnym. Problematyka ciągłości działania na styku sieci GSM, WAN, LAN – Patryk Gutowski.
9. Monitoring na potrzeby bezpieczeństwa publicznego, ratownictwa i monitorowania zagrożeń – dr inż. Jerzy Sobstel.
10. Rozwiązania sprzętowe rozpoznawania ruchu na przykładzie urządzenia TRK firmy IOImage – mgr inż. Andrzej Radoń, AKODO
11. Integratory systemów monitorujących na tle doświadczeń angielskich – mgr inż. Daniel Kamiński.
12. Bezobsługowe stacje monitorowania alarmów jako perspektywa rozwoju w Polsce. Potrzeby techniczne – Realizacja – mgr inż. Piotr Król, mgr inż. Jarosław Kurzawa.
13. Monitoring ciągłych sygnałów analogowych w zastosowaniach przemysłowych i monitorowaniu zagrożeń. Perspektywa rozwoju w Polsce – mgr inż. Mirosław Patej.
14. Nowe techniki monitorowania osób i obiektów ruchomych. Wykład połączony z prezentacją – mgr inż. Tomasz Fąfara, Keratronik.

Panel 3. Zagadnienia techniczne w monitoringu wizyjnym

15. Co ma wspólnego matematyka i fizyka z monitoringiem wizyjnym? Kamery IP a przesyłanie i magazynowanie obrazów w sieciach komputerowych – mgr inż. Andrzej Walczyk.
16. Monitoring szkół – nowe wyzwania i perspektywy ochrony obiektów publicznych przed sytuacjami kryzysowymi związanymi z zagrożeniem życia i zdrowia – dr inż. Andrzej Ryczer, mgr inż. Lech Wicherkiewicz.
17. Weryfikacja wizyjna alarmów z wykorzystaniem transmisji danych w sieciach komórkowych II i III generacji – mgr inż. Grzegorz Czamara, Orange.
18. Wizyjny monitoring inteligentny. Zastosowanie algorytmów heurystycznych do analizy obrazu w czasie rzeczywistym jako narzędzia poprawiającego jakość i skuteczność pracy operatorów systemu monitoringu wizyjnego – mgr inż. Rafał Dunal, Esaprojekt.

Osoby zainteresowane udziałem w X Forum Monitoringu Polskiego prosimy o kontakt z Biurem Zarządu Stowarzyszenia „POLALARM": polalarm@polalarm.com.pl, polalarm@alter.pl, tel./faks (0-22) 626-90-31, 625-57-43

Karta zgłoszenia udziału w X Forum Monitoringu Polskiego jest dołączona do bieżącego numeru *Zabezpieczeń* oraz jest również dostępna na stronie

http://www.zabezpieczenia.com.pl

Zapraszamy!

Bezp. inf. Polalarm

Nowa siedziba firmy SUMA

Firma **SUMA**, uznany dystrybutor rozwiązań sieciowych wideo IP, zmieniła swoją lokalizację. Nowe biuro mieści się w Katowicach, jest usytuowane blisko centrum miasta i głównych dróg dojazdowych.

Większa powierzchnia i nowoczesny wystrój nie tylko poprawią komfort pracy pracowników firmy SUMA, lecz także pozwolą bardziej profesjonalnie obsługiwać klientów.

W nowej siedzibie znalazło się także miejsce na salę konferencyjno-szkoleniową (szkolenia rozpoczną się już wkrótce).

Nowy adres firmy:
PPHU SUMA Sp. z o.o.
ul. Roździeńskiego 88a, 40-203 Katowice
nowy nr telefonu: 032 258 05 97
nowy nr faksu: 032 258 05 98

Bezp. inf. Suma

XIII Walne Zgromadzenie PISA

Prezes Zarządu utracił mandat

Przed oficjalnym otwarciem XIII Walnego Zgromadzenia Członków Polskiej Izby Systemów Alarmowych, które odbyło się 31 maja 2007 r. w Jachrance k. Warszawy, odbyło się posiedzenie wspólne Rady Nadzorczej i Zarządu PISA.

Nie byłoby w tym nic nadzwyczajnego gdyby nie fakt, że tydzień wcześniej Zarząd Izby stwierdził wygaśnięcie mandatu członka organów PISA – prezesa Zarządu **Eugeniusza Winieckiego**, który funkcję tę pełnił od 11 maja 2006 r.

Zaproszony do udziału w posiedzeniu Rady i Zarządu były prezes PISA uznał działania członków Zarządu i dyrektora Biura w jego sprawie za celowe dążenie do pozbawienia go funkcji prezesa, a samo stwierdzenie wygaśnięcia mandatu za bezpodstawne.

Żaden z członków Rady Nadzorczej i Zarządu nie podzielił poglądów E. Winieckiego. Przywołano dokumenty, w tym stosowne postanowienia statutu PISA, będące podstawą stwierdzenia wygaśnięcia mandatu, a także jednoznaczną w tym względzie opinię kancelarii prawnej.

Przekazany na ręce przewodniczącego Rady Nadzorczej list E. Winieckiego do Walnego Zgromadzenia nie był w trakcie dyskusji podczas obrad przedmiotem najmniejszego zainteresowania.

Obrady Walnego Zgromadzenia, którym przewodniczył **Georgis Bogdanis** (MICROSYSTEM z siedzibą w Sopocie), przebiegały zgodnie ze znanym wcześniej wszystkim członkom Izby, a następnie uchwalonym, projektem porządku.

W trakcie Walnego Zgromadzenia siedmiu osobom uroczyście wręczono certyfikaty eksperta i eksperta stowarzyszonego PISA w zakresie bezpieczeństwa. Osoby te złożyły również przyrzeczenie.

Status eksperta PISA otrzymali: Halina Grązka (VIDOM z siedzibą w Mińsku Mazowieckim), **Krzysztof Cichulski** (ATLine z siedzibą w Łodzi), **Waldemar Ciesielczyk** (DATEL z siedzibą w Poznaniu), a status eksperta stowarzyszonego PISA: **Marek Chrobot** (PTK Centertel z siedzibą w Warszawie), **Roman Iwanicki** (PTK Centertel z siedzibą w Warszawie), **Przemysław Kępka** (ENERGA z siedzibą w Gdańsku), **Roman Kosiński** (BGŻ – Centrala z siedzibą w Warszawie).

Dyskusja uczestników obrad koncentrowała się na sprawach związanych z nowymi uregulowaniami dotyczącymi rekomendacji technicznych PISA, objęciem zainteresowanych firm członkowskich zbiorowym ubezpieczeniem OC, udziałem w targach Securex '2008 na zapowiedzianych, preferencyjnych dla PISA warunkach, odpłatnością za udział w Walnych Zgromadzeniach, pracą nad zasygnalizowanymi zmianami w zasadach wnoszenia składek członkowskich.

W wystąpieniu gościa Walnego Zgromadzenia – **Wojciecha Dąbrowskiego** z Instytutu Mechaniki Precyzyjnej, członka Rady Programowej Ośrodka Szkoleniowego PISA – zawarty został apel o podjęcie wspólnych prac przygotowawczych do określenia – na potrzeby ubezpieczycieli – wymagań i warunków technicznych, jakie powinny być spełnione przy ubezpieczaniu obiektów chronionych systemami zabezpieczeń technicznych.

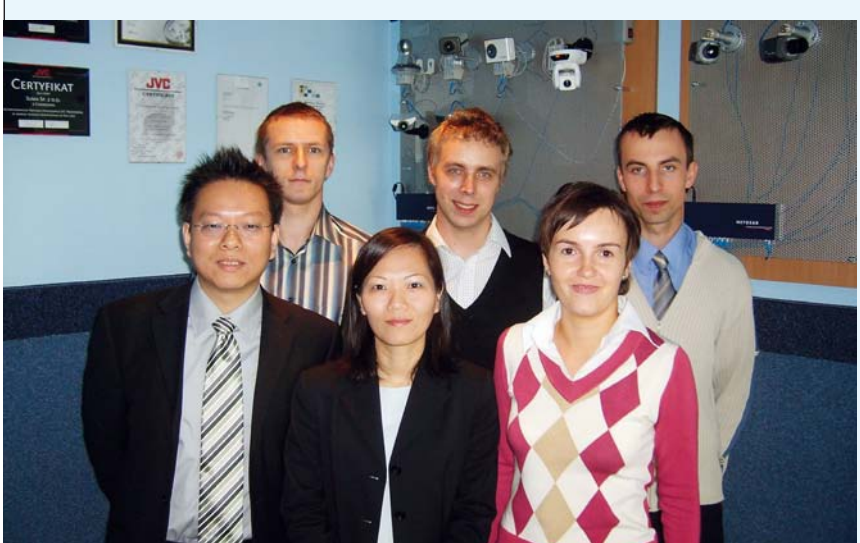
Walne Zgromadzenie udzieliło absolutorium organom PISA, przyjęło sprawozdanie finansowe za 2006 r., uchwaliło budżet Izby na 2007 r., a także kierunki jej pracy na najbliższy rok.

XIII Walne Zgromadzenie dokonało także wyboru Sądu Koleżeńskiego na trzyletnią kadencję. Arbitrami PISA w sprawach określonych w Regulaminie Sądu zostali: **Halina Grązka** (przewodnicząca), **Krzysztof Cichulski** i **Waldemar Ciesielczyk**.

Zarząd Polskiej Izby Systemów Alarmowych na posiedzeniu 13 czerwca 2007 r. powierzył funkcję prezesa Zarządu **Mirosławowi Krasnowskiemu**, a funkcję wiceprezesa **Zarządu Bogdanowi Jędrychowi**.

Biuro Polskiej Izby Systemów Alarmowych

Vivotek w Polsce



Na zdjęciu (od lewej):
Evan Chang (Vivotek), Marcin Kulik (Suma), Sharon Lee (Vivotek), Robert Stanosz (Suma), Monika Mirczewska-Stanosz (Suma), Rafał Chmielewski (Suma)

Przedstawiciele firmy **VIVOTEK**, składając wizyty robocze u europejskich dystrybutorów, zawitali również do firmy **SUMA** – reprezentującej Vivotek w Polsce.

Sharon Lee, senior manager, i Evan Chang, deputy regional manager, rozmawiali o polityce sprzedaży na polskim rynku, nowych produktach, które zostaną wprowadzone do oferty w bieżącym roku.

Wśród nowości można się spodziewać nowego darmowego oprogramowania rozszerzonego o wiele nowych funkcjonalności. Wkrótce firma wprowadzi także nowe modele kamer; statycznych i obrotowych. Zapowiada się dobry rok dla instalatorów wykorzystujących w pracy produkty firmy Vivotek.

Bezp. inf. Suma

FINNSEC 2007

Centrum Promocji Eksportu PROEXPO zaprasza Państwa do zaprezentowania oferty firmy podczas Międzynarodowych Targów Ochrony i Zabezpieczeń i BHP **FINNSEC 2007**, które odbędą się w dniach **03–05.10.2007** w Helsinkach, w Finlandii.

Targi odbywają się co dwa lata na nowoczesnych terenach targowo-wystawienniczych i rokrocznie skupiają zarówno coraz więcej wystawców, jak i samych odwiedzających. W ostatniej edycji targów, w roku 2005, zaprezentowało się 185 wystawców z kilkunastu krajów. Według oficjalnych danych odwiedziło je ponad 15000 osób, głównie specjalistów z branży. Targom towarzyszą konferencje i seminaria tematyczne. Odbywają się pod patronatem organizacji i wydawnictw branżowych.

Podstawowe zagadnienia poruszane na konferencjach podczas targów to:

– bezpieczeństwo i higiena pracy,
– ochrona przeciwpożarowa, ratownictwo,
– ochrona środowiska, zabezpieczenia,
– bezpieczeństwo w domu i na drodze,
– zarządzanie antykryzysowe,
– elektroniczne systemy zabezpieczeń,
– indywidualne akcesoria i urządzenia zabezpieczające,
– usługi w zakresie ochrony i nadzoru,
– organizacje i wydawnictwa,
– inne.

Jednocześnie informujemy, że Centrum Promocji Eksportu PROEXPO oferuje obsługę logistyczną uczestników targów.

O przydziale powierzchni wystawienniczej decyduje kolejność zgłoszeń.

Szczegółowe informacje:

Centrum Promocji Eksportu PROEXPO
ul. Hetmańska 28, pok. 311, 85-039 Bydgoszcz
tel./faks: 052 345 46 00, 052 345 43 01
e-mail: proexpo@proexpo.com.pl
Kontakt: Małgorzata Zasada

Bezp. Inf. CPE PROEXPO

Projekt ropociągu adriatyckiego

Mająca siedzibę w chorwackim Zagrzebiu firma JANAF Plc. zarządza systemem ropociągów, stanowiących nowoczesny, efektywny i oszczędny sposób przesyłu ropy naftowej. Obecnie, z pomocą integratora, przedsiębiorstwa Tehnozavod Marusic, realizuje projekt monitoringu odcinka ropociągu od granicy serbskiej do Adriatyku.

Tehnozavod zaprojektował i zainstalował system CCTV wykorzystujący technologię IP, a oparty na komponentach firmy **Videotec**. Na zrealizowany nad Adriatykiem pierwszy z pięciu etapów złożyło się 100 kamer IP w obudowach HOV, iluminatory działające w podczerwieni oraz 14 urządzeń pozycjonujących Videotec Ulisses z wbudowanym modułem kamerowym Sony, sterowane zdalnie przez serwery wideo.

Najważniejsze problemy, jakie Tehnozavod napotkał przy projektowaniu tego systemu, stanowiły wysokie temperatury w sezonie letnim oraz słynny lokalny wiatr Bora, który potrafi osiągać prędkość ponad 200 kilometrów na godzinę.

Problem pracy w lecie doskonale rozwiązały obudowy HOV firmy Videotec – dzięki wydajnemu systemowi chłodzenia temperatura wewnątrz obudowy znacznie maleje.

Z drugiej strony, urządzenia pozycjonujące z serii Ulisses charakteryzują się odpornością na statyczne podmuchy wiatru o prędkości 160 km/h, a w warunkach operacyjnych – na podmuchy do prędkości 160 km/h. Bora nie stanowi więc problemu.

Igor Benko, menedżer projektu w firmie Tehnozavod, potwierdza: „Projekt ten zdecydowanie stanowi dla nas wyzwanie. Cały system będzie składał się z ponad pięciuset nieruchomych kamer IP oraz dodatkowych stu kamer ze sterowaniem położenia i zbliżenia (PTZ), rozciągniętych między dwiema granicami kraju. Będzie to prawdopodobnie największa instalacja tego typu w Chorwacji".

Redakcja

Opracowano na podstawie materiałów firmy Videotec

Zapraszamy na seminarium

Trendy rozwojowe technicznych systemów bezpieczeństwa

Instytut Systemów Elektronicznych Wydziału Elektroniki WAT wraz z Instytutem Optoelektroniki WAT oraz niezależnym Instytutem Inżynierii Systemów Bezpieczeństwa zaprasza wszystkich absolwentów studiów podyplomowych „Techniczna ochrona osób i mienia" prowadzonych na Wydziale Elektroniki WAT w latach 1997–2007 oraz inne osoby i firmy zainteresowane tematyką bezpieczeństwa na

SEMINARIUM
„Trendy rozwojowe
technicznych systemów bezpieczeństwa"

Seminarium połączone jest ze zjazdem koleżeńskim absolwentów dziesięciu. edycji studiów podyplomowych „Techniczna ochrona osób i mienia", dla których przewidziane są dodatkowe atrakcje.

Seminarium odbędzie się w Wojskowej Akademii Technicznej w Warszawie w dniach **27–28 września 2007**.

Celem seminarium jest zapoznanie jego uczestników z obecnym stanem wiedzy na temat najnowszych trendów i rozwiązań w dziedzinie szeroko rozumianego bezpieczeństwa (zarówno w aspekcie technicznym, jak i organizacyjno-prawnym).

Szczegółowe informacje na temat seminarium (formularz zgłoszenia uczestnictwa) można znaleźć na stronach **www.wel.wat.edu.pl** i **www.i2sb.org.pl** lub uzyskać pod numerem telefonu **022 683 98 09**.

Redakcja

XI Krajowa Konferencja Kryptografii i Ochrony Informacji

ENIGMA 2007

Tegoroczna, jedenasta już Krajowa Konferencja Kryptografii i Ochrony Informacji ENIGMA 2007 odbyła się w dniach 23-25 maja 2007 roku w Warszawie, w hotelu Lord, pod honorowym patronatem Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.

W programie przewidziano 34 referaty z zakresu kryptografii, ochrony informacji i zarządzania bezpieczeństwem informacji, zaprezentowane podczas 14 sesji tematycznych. Drugiego dnia konferencji prowadzono równolegle – w toku kryptograficznym oraz organizacyjnym – po trzy sesje, z których każda obejmowała po trzy referaty. Także tego dnia zaprezentowano dokonania finalistów tegorocznej edycji konkursu prac dyplomowych, magisterskich i inżynierskich, z dziedziny kryptografii i ochrony informacji. Konkurs ten, organizowany już po raz siódmy podczas konferencji ENIGMA, ma na celu promocję ich autorów w polskim środowisku kryptograficznym. Imprezą towarzyszącą konferencji były zorganizowane 28 maja specjalistyczne warsztaty pt. *Quo vadis cryptology?* z udziałem światowej sławy ekspertów z dziedziny ataków na implementacje algorytmów kryptograficznych.

Mijający rok w kryptografii podsumował w obszernym wystąpieniu podczas pierwszej sesji prof. Krzysztof Gaj z George Mason University. W ostatnim dniu konferencji ogłosił on także wyniki konkursu prac dyplomowych, a pięcioro jego laureatów zostało uhonorowanych dyplomami i nagrodami.

Blisko połowa referatów dotyczyło zagadnień związanych z bezpieczeństwem lub ochroną informacji. W jednym z pierwszych referatów podsumowano „5 lat oficjalnego życia podpisu elektronicznego" w Polsce. Tematem innego z tej grupy sesji były metody zabezpieczania transmisji skompresowanych danych multimedialnych, m.in. szyfrowania danych wideo i audio. Kilka referatów dotyczyło bezpieczeństwa przesyłania danych za pośrednictwem sieci, w tym pakietowych sieci bezprzewodowych różnego rodzaju. Jak dobrze sprzedawać bezpieczeństwo stronie biznesowej to podtytuł referatu poświęconego zależnościom pomiędzy bezpieczeństwem IT a wartością przedsiębiorstwa, dedykowanego kadrze zarządzającej przedsiębiorstw. W jednym z referatów przedstawiono założenia nowego standardu ISO, dotyczącego zasad budowy i utrzymania w działaniu zapasowych centrów przetwarzania informacji. W kilku referatach omówiono zagadnienia związane z normami i certyfikatami, istotnymi w zarządzaniu bezpieczeństwem informacji.

Warto podkreślić wysoki poziom przedstawionych referatów i udział w konferencji specjalistów z dziedziny kryptografii nie tylko z naszego kraju, ale także reprezentujących renomowane ośrodki naukowe z różnych kontynentów.

Adam Bułaciński

Centra miast stosują kamerę

Metal Mickey

do tworzenia wszechstronnych i wytrzymałych rozwiązań CCTV

Zarządzający bezpieczeństwem w centrum brytyjskiego miasta Swindon stworzyli unikatowe rozwiązanie pozwalające na szybkie rozmieszczenie urządzeń wizyjnych. System wykorzystuje kamery MIC1-400 firmy **Forward Vision** o wdzięcznym przydomku Metal Mickey.

Współpracując z firmą instalacyjną ATEC, organizacja Swindon Crime Reduction Partnership opracowała kamerowy zestaw przenośny, który można zainstalować w ciągu godziny, jeżeli zajdzie taka potrzeba.

Zestaw ten rozstawia się na płaskich dachach sklepów lub innych budynków w centrum. Kamery MIC1-400 ustawione są tak, aby obiektywy wystawały tuż ponad krawędź dachu, zapewniając dyskretną i skuteczną obserwację rejonu poniżej. Każdy zestaw posiada baterię gwarantującą 24-godzinną transmisję obrazów do odbiornika, umieszczonego na dachu 23-piętrowego budynku władz miejskich. Jednostki mają zasięg do trzydziestu kilometrów, a więc możliwa jest również obserwacja rejonów znacznie oddalonych od centrum miasta.

Kamery MC1-400 zostały wybrane przez Olivera O'Della, dyrektora organizacji Swindon Crime Reduction Partnership, ze względu na ich wytrzymałą konstrukcję.

Wiele razy korzystałem z kamer w kwadratowych obudowach i uznałem, że są bardzo podatne na uszkodzenia. W ciągu roku straciłem sprzęt o wartości 35 000 tysięcy funtów z powodu, uderzeń, miotania cegłami oraz strzałów kulkami łożyskowymi. Często dochodziło również do niszczenia okablowania. Kamery Metal Mickeys są wystarczająco wytrzymałe, aby wyjść cało z takiej opresji. Dlatego można z nich korzystać w każdej sytuacji – mówi.

Główną zaletą stosowania nowych kamer przenośnych jest to, że przestępcy nie będą mogli przyzwyczaić się do ich położenia. Stale będą musieli zgadywać, skąd są obserwowani.

W przeszłości korzystałem z kamer zamontowanych na stałe w określonych miejscach i zauważyłem, że incydenty najczęściej zdarzają się tuż poza granicą zasięgu urządzeń. Przestępcy potrafią bardzo sprytnie unikać kamer, ale przemieszczając kamery z dachu na dach możemy ich przechytrzyć – twierdzi O'Dell.

Kamera MIC1-400 uznawana jest za jedno z najbardziej odpornych i wszechstronnych urządzeń PTZ opracowanych dotychczas. Stanowi doskonałe rozwiązanie właśnie w zestawach ruchomych i zastosowaniach podobnych do opisanego. Jej korpus wykonano z aluminium o grubości 6 mm, a całe urządzenie dostępne jest w dwóch wariantach montażu.

Istotne były dla nas również dobre właściwości obserwacji nocnej, wykazywane przez kamerę MIC1-400 – dodaje Oliver O'Dell. *Dzięki urządzeniom Metal Mickey możemy teraz prowadzić monitoring centrum miasta 24 godziny na dobę*.

Redakcja

Opracowano na podstawie materiałów firmy Forward Vision

Nagroda dla kamery kopułkowej WV-CW960 firmy Panasonic

Panasonic System Solutions Europe informuje, że wyposażona w technologię Super Dynamic III kolorowa kamera kopułkowa **WV-CW960** otrzymała nagrodę PSI Premier Award oraz tytuł **Produktu Roku 2007** w dziedzinie CCTV.

Wręczenie nagród odbyło się 5 czerwca w Moor Park Golf Club w angielskim hrabstwie Hertfordshire. Jako gospodarze wystąpili członkowie kolegium redakcyjnego Pro-Activ Publications. Nagrody stanowiły uhonorowanie firm, które przez ostatni rok osiągnęły doskonałość w różnorodnych dziedzinach.

Redakcja

Opracowano na podstawie materiałów firmy Panasonic

Fundacja Pomocy Pracownikom Ochrony i Ich Rodzinom **„Ochrona i Pomoc”**

Powołanie przez Polską Izbę Ochrony Osób i Mienia Fundacji Pomocy Pracownikom Ochrony i Ich Rodzinom „Ochrona i Pomoc” jest realizacją uchwały numer 1 Zarządu Izby podjętej 4 stycznia 2007 roku. Jej celem było objęcie realną i szeroką opieką znajdujących się w trudnej sytuacji życiowej pracowników branży ochrony oraz ich rodzin.

Fundacja została zarejestrowana 17 kwietnia 2007 roku w Sądzie Rejonowym dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, i wpisana do Rejestru Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji oraz Publicznych Zakładów Opieki Zdrowotnej pod numerem KRS 0000278664.

Fundacja oraz PIOOiM mają wspólną siedzibę w Warszawie, przy ul. Kasprzaka 29/31 lok. 203. Zgodnie ze Statutem, podstawowym celem działalności Fundacji będzie udzielanie pomocy pracownikom branży ochrony i ich rodzinom, znajdującym się w trudnej sytuacji życiowej.

Cele te realizowane będą poprzez:

- udzielanie zapomóg materialnych i finansowych ofiarom wypadków poszkodowanym podczas wykonywania zadań ochrony, rodzinom pracowników ochrony znajdującym się w trudnej sytuacji życiowej w celu wyrównywania ich szans życiowych,
- dofinansowanie kosztów kształcenia pracowników ochrony i ich dzieci,
- organizowanie kolonii i obozów dla dzieci i młodzieży z rodzin pracowników ochrony lub dofinansowanie ich pobytu na wypoczynku organizowanym przez inne instytucje czy organizacje,
- prowadzenie poradnictwa na rzecz pracowników ochrony i ich rodzin.

Fundacja nie prowadzi działalności gospodarczej, a założone cele może realizować jedynie ze środków pochodzących z:

– darowizn od osób prawnych i fizycznych,
– zbiórek publicznych,
– spadków i zapisów na rzecz Fundacji.

Fundacja, powołana przez Polską Izbę Ochrony Osób i Mienia, swoją opieką pragnie objąć pracowników firm zrzeszonych w PIOOiM i ich rodziny, ale będzie również udzielać pomocy pozostałym pracownikom branży ochrony. Szczególną troską otoczeni zostaną pracownicy, poszkodowani podczas wykonywania służbowych zadań związanych z ochroną osób i mienia, oraz ich rodziny bez względu na przynależność do PIOOiM.

Członkowie Rady i Zarządu prowadzą własną działalność gospodarczą i zawodową, a pracę na rzecz Fundacji wykonują w ramach społecznego zaangażowania, bez pobierania wynagrodzenia.

Zapraszamy do współpracy!

Bezp. inf. PIOOiM

Kursy OS PISA

Ośrodek Szkoleniowy PISA zaprasza na kursy i seminaria organizowane w II półroczu 2007 r.:

- Kurs projektowania systemów zabezpieczeń technicznych w klasach SA1–SA4, w terminach: 17–22 września, 12–17 listopada 2007 r.
- Kurs instalowania i konserwacji systemów zabezpieczeń technicznych w klasach SA1–SA4, w terminach: 15–19 października, 10–14 grudnia 2007 r.
- Kurs inwestorów systemów zabezpieczeń technicznych, w terminie: 26 – 30 listopada 2007 r.
- Seminaria projektowe
- Seminaria instalacyjne
- Kurs ekspertów w zakresie bezpieczeństwa – w przygotowaniu
- Kurs kosztorysowania systemów zabezpieczeń technicznych – w przygotowaniu

Absolwenci kursów otrzymują dokumenty wystawiane bezterminowo: zaświadczenie ukończenia kursu (druk MEN) oraz dyplom Ośrodka Szkoleniowego PISA.

Szczegółowe informacje:
OS PISA
tel. (022) 620-45-57,
faks (022) 654 57 32,
www.pisa.org

Zapraszamy do skorzystania z naszej oferty.

Bezp. inf. Ośrodek Szkoleniowy PISA

Konferencja IDC Storage & Datacenters Roadshow 2007

Jednym z jedenastu miast europejskich, w których wiosną 2007 roku odbywały się konferencje IDC poświęcone przechowywaniu i ośrodkom danych, była Warszawa. Polska konferencja **IDC Storage & Datacenters Roadshow 2007** została zorganizowana przez IDC oraz jej następujących partnerów: Cisco, HP, APC-MGE, S&T, VMWare, EMC i odbyła się 22 maja 2007 roku w warszawskim hotelu Mariott.

Specjaliści z ww. firm, pochodzący z różnych krajów, zaprezentowali podczas konferencji referaty, które były związane z jednym z najistotniejszych problemów naszych czasów: nadmiarem danych. Zdaniem p. Jensa Leischnera, doświadczonego eksperta w dziedzinie planowania sieci przechowywania danych (SAN – od ang. *Storage Area Network*) oraz ich zarządzania, a także założyciela SANBoard – organizacji użytkowników pamięci masowych – powodem ciągłego zwiększania się ilości przechowywanych danych jest ich zła archiwizacja.

Duże ilości danych wymagają nie tylko nośników danych o ogromnych pojemnościach, lecz także właściwej budowy ośrodków danych, tak aby przetwarzające je organizacje mogły zapewnić zarówno kontrolę nad przechowywaną informacją, jak i jej bezpieczeństwo (jak powiedział przedstawiciel IDC Poland, p. Jarosław Smulski – „zachować wszystko, zachowując kontrolę nad pamięciami masowymi"). Ważne jest zarówno przemyślane rozmieszczenie urządzeń, uwzględniające ilości ciepła, wydzielanego przez nie, jak i wybór odpowiedniego rozwiązania pamięci masowej.

Coraz bardziej istotny staje się problem zwiększającego się zużycia energii elektrycznej, przeznaczanej do zasilania systemów informatycznych przedsiębiorstw, zwłaszcza tych o rozbudowanej strukturze organizacyjnej. Zgodnie z prognozą, przedstawioną przez p. Macieja Bociana z Cisco, „za trzy lata 50 proc. firm będzie mieć wyższe wydatki na energię elektryczną niż na inne cele". Rozwiązaniem, które prowadzi do ograniczenia związanych z tym kosztów, jest wirtualizacja systemów informatycznych, czyli zastosowanie specjalistycznego oprogramowania sieciowego, mającego na celu optymalizację wykorzystania posiadanego przez firmę sprzętu.

Wirtualizacja pozwala na zmniejszenie liczby sprzętu informatycznego, niezbędnego do prowadzenia przez firmę działalności (jest on z reguły, pod względem mocy obliczeniowej, wykorzystywany w niewielkim procencie) i na efektywne zarządzanie zasobami pamięciowymi. Według p. Macieja Ostrowskiego z firmy VMWare „wykorzystanie wirtualizacji dla zapewnienia ciągłości biznesowej pozwala w prostszy sposób zapewnić bezpieczeństwo większej liczbie aplikacji przy jednoczesnym zredukowaniu czasu odtwarzania po awarii".

Adam Bułaciński

Mic1-400 *kontra* wąż strażacki

Metal Mickey stawia czoło nawet potopowi... urządzonemu przez strażaków

Kamera Mic1-400 firmy **Forward Vision** przeszła niedawno test wytrzymałości na działanie wody pod ekstremalnie wysokim ciśnieniem Miał on pokazać, że rzeczywista odporność urządzenia znacznie przekracza dane ujęte w specyfikacji. Urządzenie wykonane z aluminium o grubości 6 mm lub ze stali nierdzewnej 316L posiada klasę szczelności IP68. Oznacza to, że jest w stanie znieść bez uszkodzenia zanurzenie w wodzie. Zapewnia to niezawodne działanie w najbardziej ekstremalnych warunkach, takich jak uderzenie strumienia wody pod wysokim ciśnieniem.

Dzięki unikatowej konstrukcji produkt Extreme CCTV doskonale nadaje się do ochrony portów oraz nabrzeży. Kamery Mic1-400 zostały już zainstalowane w wielu szczególnie ważnych obiektach na świecie: w brytyjskim systemie tranzytowym, na mostach, w tunelach oraz w londyńskim metrze. Test przeprowadzono we współpracy z jednostką straży pożarnej nr 1 z kanadyjskiego miasta Barnaby.

Redakcja

Opracowano na podstawie materiałów firmy Forward Vision

Konferencja MUZ w Mościskach

25 maja br. w Mościskach, w firmie Kłos (producent zamków i urządzeń bankowych), odbyła się druga część konferencji „Działania firmy MAUER z grupy KABA dla bezpieczeństwa osób i mienia", z cyklu poświęconego wytwórstwu i dystrybucji mechanicznych urządzeń zamykających w kraju.

Obecni na spotkaniu członkowie Sekcji MUZ i zaproszeni goście po omówieniu przez Prezesa Sekcji MUZ spraw stowarzyszeniowych zapoznali się z produktami firmy Kłos, wyposażanymi w różne rodzaje zamków, w tym przede wszystkim firmy Kaba Mauer, prezentowanymi przez Zbigniewa Kłosa.

Wytwórnia oferuje duży asortyment produktów, takich jak np. dyspensery z zamkniętym obiegiem banknotów, multisejfy, wrzutnie nocne i zestawy wrzutowe, szafy transferowe, zamki zabezpieczeniowe, mechaniczne kluczowe, kodowe sterowane mechanicznie i elektronicznie, bezpośredniego ryglowania (sprzęgające ryglami skrzydło drzwi z ościeżnicą) i współpracujące z mechanizmami blokującymi drzwi skarbcowych i szaf do przechowywania wartości, w tym wszystkie modele zamków i akcesoriów Kaba Mauer (zapewnia również serwis urządzeń).

Szczegółowo omówiono wszystkie funkcje sterowanego elektronicznie zamka kodowego SL 523 i 525 firmy Kaba Mauer, posiadającego certyfikat klasy „B" w klasyfikacji zamków skarbcowych, wyróżniającego się prostą, niezawodną konstrukcją oraz łatwym i szybkim montażem i mającego zastosowanie we wszelkiego typu pomieszczeniach i urządzeniach do przechowywania i transportowania wartości.

Następna konferencja z ww. cyklu planowana jest we wrześniu.

Opracował: Józef Rudziński
Prezes Sekcji MUZ przy ZG SIMP

SpeedDome Ultra VIII

NOWOŚĆ WŚRÓD PROGRAMOWALNYCH KAMER KOPUŁKOWYCH

Firma **ADT** wypuściła na rynek najnowszą wersję kamer szybkoobrotowych **SpeedDome**. W sprzedaży w Polsce będą dostępne dwie wersje SpeedDome Ultra VIII: z 22- i z 35-krotnym zoomem optycznym. Obie posiadają znaczące udoskonalenia w porównaniu z wcześniejszymi modelami, zwłaszcza pod względem jakości obrazów, jak również programowania i sterowania urządzeniem, instalacją oraz konfiguracją.

Kamery SpeedDome charakteryzują się zaawansowanymi funkcjami do programowania i zarządzania, umożliwiającymi stały ruch obrotowy w zakresie 360° oraz panoramowanie spiralne. Seria 35x oferuje 420-krotne powiększanie obrazu dzięki 35-krotnemu zoomowi optycznemu z 12-krotnym powiększeniem cyfrowym. Seria 22x posiada możliwość 242-krotnego powiększania obrazu, na które składa się 22-krotny zoom optyczny i 11-krotne powiększenie cyfrowe, co daje doskonałą jakość i zapewnia duży poziom szczegółowości obrazu.

Seria 35x zawiera także nowy system stabilizacji obrazu, który pomaga redukować efekt wibracji spowodowany warunkami pogodowymi, takim jak np. wiatr. Ponadto, dzięki funkcji Dzień/Noc oraz technologii cyfrowego spowalniania migawki (DSS), seria 35x pozwala użytkownikom wyraźnie widzieć obrazy nawet przy oświetleniu tak słabym, jak 0,00041 luksa, czyniąc z niej idealne rozwiązanie dla obserwacji na zewnątrz i wewnątrz budynków.

Kolejną cechą serii 35x jest jej nowa obudowa ze wskaźnikiem temperatury i wilgotności powietrza oraz możliwością szybszego poruszania się. Kamera może wykonywać obrót do 360° w ciągu sekundy, w porównaniu z 220° na sekundę w starszych modelach.

Zarówno SpeedDome Ultra VIII seria 35x, jak i seria 22x obsługują do 96 zaprogramowanych ustawień zdefiniowanych przez użytkownika oraz posiadają funkcję Pozycji wyjściowej. Dzięki niej można ustawić dla kamery zaprogramowane położenie albo domyślny tor obserwacji, do którego ma powracać w czasie, gdy nie jest używana. Można też zdefiniować do ośmiu stref prywatnych w celu uniemożliwienia użytkownikom dostępu do obrazów z obszarów zastrzeżonych.

– *SpeedDome Ultra VIII tworzy statystyki wykonanych ruchów panoramowania, powiększania i pochylania, dostarczając informacji o tym, jak często obszar jest kontrolowany. Ma też funkcje takie jak: poszerzenie zakresu dynamiki, praca w podczerwieni, ochrona dostępu za pomocą hasła oraz wyświetlanie generowanego tekstu na ekranie. Kamera SpeedDome Ultra VIII posiada nowatorski mechanizm mocowania w podstawę montażową („wkręć, zamocuj, puść") w celu łatwej instalacji i konserwacji. To jeszcze bardziej poszerza zakres rozwiązań w dziedzinie elektronicznych zabezpieczeń oferowanych naszych klientom* – mówi Agnieszka Dąbrowska, product manager CCTV w ADT.

Bezp. inf. ADT Polska

Axis 211 M – diabeł tkwi w szczegółach

Nowa megapikselowa kamera **Axis** została zaprojektowana do zastosowań w miejscach, w których niezbędna jest precyzyjna identyfikacja monitorowanych obiektów. Dzięki kamerze **211 M** otrzymają Państwo wyraźny obraz wszystkich interesujących was detali.

Kamera Axis 211 M nie tylko dostarcza obraz o rozdzielczości 1,3 megapiksela pozwalający na uzyskanie 4-krotnie większej szczegółowości, ale także oferuje wiele funkcji dodatkowych. Progressive Scan to nowoczesna technika skanowania obrazu zapewniająca niezwykłą ostrość obrazu rzeczy lub osób znajdujących się w ruchu, np. wchodzących i wychodzących ludzi. Kamera może jednocześnie obsługiwać formaty Motion JPEG i MPEG-4.

Dodatkowo, dwukierunkowa obsługa audio umożliwia nie tylko odsłuchiwanie dźwięku z chronionego obszaru, lecz także przekazywanie komunikatów obsługi czy ochrony. Nowe urządzenie może być zasilane poprzez sieć Ethernet w standardzie PoE (ang.: *Power over Ethernet*).

Autoryzowanym dystrybutorem marki Axis w Polsce jest Softex Data.

Bezp. inf. Softex Data

Kamery REG firmy Derwent rozmieszczone na wyścigach konnych

Kamery typu **REG** firmy **Derwent**, odczytujące numery rejestracyjne pojazdów, zostały użyte w celu poprawy bezpieczeństwa w czasie dorocznego festiwalu jeździeckiego w Cheltenham.

Dualne kamery typu REG w czasie dwudniowego festiwalu wychwyciły tablice rejestracyjne ponad 15 000 pojazdów.

„Nasi inżynierowie byli w stanie bardzo szybko uruchomić system, gdyż te kamery są kamerami typu *plug and play*"– wyjaśnia Don Wetherell z firmy Special Events Communications. „Dane o numerach rejestracyjnych zostały przesłane za pomocą skrętki NVT do stanowiska policyjnego. Z punktu kontrolnego mogliśmy monitorować różne miejsca, które znajdowały się w odległości nawet 600 metrów".

„Przy wydarzeniach tego typu jak ten festiwal nie ma miejsca na błąd" – wyjaśnia Don Wetherell. „Urządzenia, których używamy, muszą zawsze pracować od momentu ich włączenia i musimy wiedzieć, że możemy na nich polegać".

Dualne kamery firmy Derwent typu REG Dual zapewniają zintegrowane rozpoznawanie numerów rejestracyjnych pojazdów niezależnie od oświetlenia i warunków pogodowych. Wysokiej rozdzielczości kolorowa kamera zapewnia podgląd otoczenia, uwzględniając kształt pojazdów, ich markę i kolor.

Redakcja

Opracowano na podstawie materiałów firmy Derwent

Extreme CCTV

zapewni monitoring w ośrodkach poprawczych dla młodzieży

Kamera firmy **Extreme CCTV** o oznaczeniu **EX36** posłuży do nadzoru osadzonych w ośrodkach poprawczych na południu Stanów Zjednoczonych. Urządzenie to zostało zaprojektowane z myślą o instalacjach więziennych i tym podobnych – montuje się je w narożniku pomieszczenia. Przylega ono bardzo ściśle do ścian i sufitu, co uniemożliwia jego wyrwanie. Kąt widzenia wynosi 45 stopni; gwarantuje to obserwację całego pomieszczenia, także obszaru bezpośrednio pod kamerą. Masywna obudowa oraz wizjer zabezpieczony płytą wykonaną z leksanu czynią kamerę odporną na próby zniszczenia, usunięcia lub wykorzystania do samookaleczenia.

FAKTY:

1. Kształt spłaszczonego stożka sprawia, że EX36 pasuje do montażu w narożnikach pomieszczeń.
2. Posiadającą amerykańskie patenty kamerę EX36 instaluje się w więzieniach w USA, w Kanadzie, w Wielkiej Brytanii, w Australii oraz w Nowej Zelandii.
3. EX36 umożliwia obserwację w ciemności, gwarantując ochronę przed próbami samobójczymi osadzonych.
4. Kamera EX36 jest tak wytrzymała, że opiera się nawet najbardziej zaciekłym próbom zniszczenia.
5. Federalne Biuro Więziennictwa wybrało EX36 do instalacji w amerykańskich więzieniach o najostrzejszym rygorze.

ZASTOSOWANIE:

1. Cele więzienne.
2. Pomieszczenia szpitalne.
3. Pomieszczenia w ośrodkach psychiatrycznych.
4. Rejony zagrożone wandalizmem.

Redakcja

Opracowano na podstawie materiałów firmy Derwent

Najnowszy bezprzewodowy system Visonic

POWER MAX PRO

Seria systemów bezprzewodowych **PowerMax** jest obecna na polskim rynku już od kilku lat. Centrale tej serii zmieniły rynek. W projekcie na pierwszym miejscu postawiono funkcjonalność dla użytkownika systemu. Dlatego też systemy PowerMax wyposażone są w procesor głosu. Centrala porozumiewa się z użytkownikiem głosowo w jednym z wielu dostępnych języków, także po polsku. Pierwszy model PowerMax został zainstalowany w przeszło 500 tysiącach obiektów. Potężne doświadczenie zarówno projektantów, jak i instalatorów systemu dało podstawę do nowych projektów. Kolejnym krokiem był PowerMax PLUS. Idea firmy ciągłego usprawniania i unowocześniania swoich systemów przyniosła zamierzony efekt. Wprowadzono wiele ciekawych rozwiązań i nowych urządzeń (m. in. dwukierunkowe bezprzewodowe klawiatury z wbudowanym wyświetlaczem LCD i procesorem głosu oraz bezprzewodowe dwukierunkowe zewnętrzne sygnalizatory). Kolejnym przełomem jest centrala PowerMax PRO. Specjalna wersja systemu z częstotliwością 868 MHz otwiera nowy rynek dla systemów bezprzewodowych, nowoczesny design – elegancka srebrna obudowa i błękitny wyświetlacz LCD przyciąga oko. Proces instalacji został maksymalnie uproszony poprzez modułową budowę, wprowadzono system partycji, co czyni system jeszcze bardziej nowoczesnym i elastycznym.

Centralę, która w podstawowej wersji posiada czytnik zbliżeniowy, można dodatkowo wyposażyć w moduły przekaźników do monitoringu, wewnętrzny lub zewnętrzny nadajnik GSM oraz moduł PowerLink umożliwiający podłączenie do Internetu. Najnowsza wersja PowerMax PRO, podobnie jak poprzednie wersje PowerMax, posiada certyfikat TECHOMU klasy C.

Bezp. inf. Visonic

Monitory plazmowe serii 600

Monitory plazmowe PELCO serii 600 charakteryzują się wyjątkową jakością obrazu (HD), wierną reprodukcją kolorów i detali oraz szerokimi kątami widzenia. Funkcja Pixel shift zapewnia długi czas eksploatacji przy obserwacji obrazów statycznych. Niewielka głębokość obudowy (około 11 cm) pozwala zaoszczędzić wiele miejsca.

Oferowane są modele o trzech przekątnych ekranu: 42, 50 i 60 cali (odpowiednio: PMCP642, PMCP650, PMCP660). Monitory są zgodne z normą EN50-130-4 wymaganą dla urządzeń przeznaczonych do systemów zabezpieczeń.

Podstawowe parametry:

- proporcje obrazu – 16:9;
- kąt widzenia – 160°;
- rozdzielczość – 1024x768 XGA (PMCP642) albo 1366x768 WXGA (PMCP650, PMCP660);
- kontrast i jasność – 8000:1, 1200 cd/m^2 (PMCP642), 8000:1, 1000 cd/m^2 (PMCP650), 6000:1, 1000 cd/m^2 (PMCP660).

Bezp. inf. Pelco

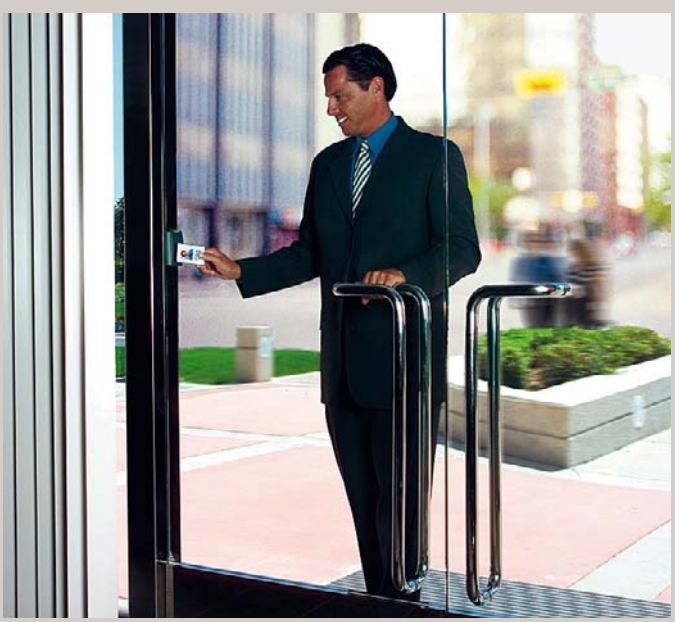
Nexus startuje z systemem Vault

Nexus, przodujący dostawca rozwiązań z zakresu cyfrowej identyfikacji i bezpieczeństwa informacji, wprowadził ostatnio rozwiązanie o nazwie Vault, obsługiwane przez technologię iCLASS firmy **HID Global**. Umożliwia ono użycie jednej bezstykowej karty do wielu różnych zastosowań związanych z kontrolą dostępu. System Vault wykorzystuje zbiór zakodowanych na karcie danych i może służyć do potwierdzenia tożsamości użytkownika karty, zapewnić dostęp do sieci lub być wykorzystany w wielu innych zastosowaniach z dziedziny bezpieczeństwa.

Vault zapewnia integrację fizycznej kontroli dostępu z logowaniem do sieci komputerowej i daje klientowi następujące korzyści:

- jedna, tania karta z zestawem zakodowanych danych, która może być stosowana w różnych celach,
- niższy koszt szkoleń i obsługi telefonicznej klienta,
- niskie koszty utrzymania.

Peter Gille – szef firmy Nexus – powiedział: „To opracowanie daje klientom firmy HID okazję do rozszerzenia możliwości dotychczas użytkowanych systemów o kontrolę dostępu do sieci komputerowej i dostarcza przyszłym klientom nieodparty powód, aby wybrali technologię iClass".



Redakcja

Opracowano na podstawie materiałów firmy HID

Sieciowe systemy kamerowe Camclosure IP

Obudowa Camclosure IP podłączana jest bezpośrednio do sieci Ethernet. Do wyboru jest osiem kombinacji kamer i obiektywów, które mogą być zainstalowane na płycie tylnej obudowy Camclosure IP. Urządzenie jest również kompatybilne z sieciowym systemem Endura produkcji **Pelco**. Zawiera własny koder i zasilacz, a obudowa jest odporna na próby manipulacji. Obsługa może odbywać się przez zewnętrzne oprogramowanie lub przeglądarkę internetową. Seria IP110 Camclosure dzięki dużemu wyborowi kamer i obiektywów, umożliwia stosowanie technologii WDR (szeroki zakres dynamiki) dzień–noc/kolor oraz uzyskanie wysokiej rozdzielczości obrazu dzień–noc/kolor. Koder wytwarza trzy jednoczesne strumienie wideo, dwa MPEG-4 (25 obrotów/s) oraz MJPEG. Obraz wideo można oglądać przy użyciu standardowej przeglądarki internetowej. Bezpieczeństwo zapewnia wielopoziomowy system dostępu. Camclosure IP może również pracować w systemie Endura, gdzie ma dostęp do technologii EnduraStor i EnduraView.

Redakcja

Opracowano na podstawie materiałów firmy Pelco

Nowa wersja oprogramowania układowego do sieciowych urządzeń wizyjnych firmy Bosch

Zalety nowej wersji oprogramowania:
1. Elastyczne profile zapisu ustawiane niezależnie dla każdej kamery.
2. Inteligentne funkcje z rozszerzoną funkcjonalnością wizyjnej detekcji ruchu (ang.: *Video Content Analysis* – VCA)
3. Wyższy poziom bezpieczeństwa z ulepszonym szyfrowaniem.

Firma **Bosch Security Systems** ogłosiła ostatnio wyprodukowanie nowej wersji oprogramowania układowego do swoich wizyjnych produktów sieciowych. Dążenie do największej możliwej funkcjonalności produktów sieciowych CCTV jest już tradycją. Nic więc dziwnego, że oprogramowanie układowe w wersji 2.5 (*Firmware Release 2.5*) obsługuje wiele rozszerzeń, łącznie z nowym harmonogramem zapisu z elastycznymi ustawieniami profili, dodatkiem do zaawansowanych funkcji oprogramowania wizyjnej analizy obrazu (VCA) oraz wyższym poziomem bezpieczeństwa możliwym dzięki zaawansowanym technikom kodowania.

Nowy harmonogram zapisu w oprogramowaniu, wersja 2.5, umożliwia ustawienie nawet dziesięciu niezależnych profili zapisu oraz przypisanie ich do poszczególnych kamer. Możliwe jest np. konfigurowanie harmonogramu z wybranymi profilami zapisu dla różnych przedziałów czasu w ciągu dnia oraz przypisanie różnych harmonogramów do wybranych dni tygodnia. Harmonogram umożliwia również ustawienie w każdym z profili zapisu trybów zapisu przed wystąpieniem alarmu i po nim. Tak więc w przypadku wyzwolenia alarmu kamery obserwujące scenę mogą automatycznie przełączyć się w tryb zapisu o większej rozdzielczości i częstotliwości odświeżania w celu uchwycenia większej liczby szczegółów zdarzenia (np. z trybu zapisu przed wystąpieniem alarmu – 1CIF przy 1 obrazie/s – do trybu po wystąpieniu alarmu 4CIF przy 25–30 obrazach/s).

Oprogramowanie układowe w wersji 2.5 zawiera również opcję inteligentnej wizyjnej detekcji ruchu wymagającą licencji na użytkowanie (IVMD 2.0, z ang.: *Intelligent Video Motion Detection*), najnowszej wersji oprogramowania VCA firmy Bosch. Oprogramowanie IVMD 2.0 oferuje wszystkie funkcje wcześniejszych wersji, łącznie z zaawansowanym algorytmem uczenia się otoczenia. Algorytm ten zapobiega fałszywym alarmom wywoływanym np. przez poruszające się gałęzie, chmury, cienie oraz opady deszczu czy śniegu, ponieważ może dostosować się do zmian otoczenia. Oprogramowanie VCA oferuje również nowe, wszechstronne funkcje: identyfikację obiektów przez współczynnik położenia, wykrywanie obiektów nieruchomych i wykrywanie usunięcia obiektów oraz wykreślanie trajektorii służącej do wykrywania podejrzanego zachowania (np. kluczenie w okolicy obszaru strzeżonego).

Nowa wersja oprogramowania zapewnia również wysoki poziom bezpieczeństwa dzięki szyfrowaniu SSL (56-bitowe DES) przy przeglądaniu stron WWW oraz połączeniom z systemami zarządzania obrazem. Aby jeszcze bardziej zwiększyć bezpieczeństwo dostępu, porty HTTP, HTTPS, telnet i RCP+ mogą być niezależnie konfigurowane lub nawet blokowane. Wersja ta obsługuje również autoryzację w standardach 802.1x, umożliwiając administratorowi systemu uwierzytelnianie urządzeń dołączonych do sieci bezprzewodowej za pośrednictwem np. serwera RADIUS.

Zaawansowane funkcje serwera czasu obejmują możliwość zmiany czasu (z edytowalną tabelą zmiany czasu) oraz obsługę protokołu SNTP i serwerów czasu RFC868. Po wybraniu protokołu SNTP dokładność czasu osiąga niespotykaną wartość 0,25 mikrosekundy, co zapewnia najwyższą dokładność synchronizacji czasu np. pomiędzy sygnałami wizyjnymi i fonicznymi.

Wskaźnik wydajności procesora obrazuje moce przerobowe dostępne dla analizy zawartości obrazu (VCA) i innych funkcji systemowych a Strona konfiguracji obrazu bieżącego wyświetla trajektorie VCA na obrazie bieżącym wraz ze standardowymi metadanymi VCA. Dostępny jest również filtr dolnoprzepustowy. Nie doprowadza on do zakłóceń mogących powstawać, gdy korzysta się z niektórych innych kamer.

Oprogramowanie układowe w wersji 2.5 jest już dostępne do użytku we wszystkich wizyjnych produktach sieciowych firmy Bosch IP, łącznie z nadajnikami VIP X1600 i sieciowymi kamerami serii FlexiDome IP.

Bezp. inf. Robert Bosch Security Systems

Lusterko z GPS-em

Firma **Cheetah** wyprodukowała lusterko wsteczne wyposażone w GPS. GPSMirror ustala pozycję samochodu i porównuje ją z mapą czarnych punktów – miejsc, w których najczęściej dochodzi do wypadków.

Kierowca jest informowany o zbliżaniu się do takiego miejsca sygnałem dźwiękowym lub wizualnym. Lusterko pokryte powłoką antyodblaskową połączone jest z odbiornikiem GPS SiRF Star. Oprócz listy niebezpiecznych miejsc w bazie danych przechowywane są także informacje o fotoradarach.

Lusterko z GPS-em potrafi również wyświetlać kierunek i prędkość pojazdu, alarmując użytkownika o zbyt szybkiej jeździe.

Źródło: Engadget

Nowe trendy i rozwiązania w dziedzinie wyświetlania obrazu

Na spotkaniu prasowym firmy **NEC Display Solutions Europe**, które 29 maja br. zorganizowała w Warszawie agencja 4D Media Relations, nowości w dziedzinie wyświetlania obrazu przedstawił p. Mariusz Orzechowski, od kilkunastu lat odpowiedzialny za sprzedaż produktów NEC – obecnie w Polsce, Czechach, Słowacji i na Węgrzech. Po jego wystąpieniu odbyła się prezentacja wybranych rozwiązań, z udziałem specjalistów z polskiego przedstawicielstwa NEC Display Solutions Europe, którego szefem jest p. Orzechowski, oraz z firm, zajmujących się dystrybucją produktów NEC w Polsce.

Na wstępie p. Orzechowski omówił zmiany organizacyjne, które nastąpiły wiosną tego roku w grupie firm NEC Corporation. Firma NEC Display Solutions Europe powstała 1 kwietnia br. z połączenia NEC Viewtechnology, działającej na rynku wideoprojektorów, oraz NEC Display Solutions, zajmującej się monitorami LCD. W ten sposób w ofercie tej nowej firmy znajdują się monitory LCD, monitory plazmowe oraz projektory, a więc wszystkie urządzenia związane z wyświetlaniem obrazu.

Jeden z trendów w dziedzinie wyświetlania obrazu dotyczy tzw. panoramicznej rewolucji i przejawia się coraz powszechniejszym stosowaniem ekranów panoramicznych – o formacie 16:10. W ubiegłym roku takie ekrany miało 70 proc. laptopów, przewiduje się, że w bieżącym będzie ich o 20 proc. więcej. Wśród monitorów LCD na uwagę zasługuje 26-calowy model z kalibracją sprzętową NEC SpectraView LCD2690 zaprojektowany dla aplikacji zarządzania kolorem, do zadań takich jak edycja obrazów i przygotowywanie materiałów do druku.

Inny nowy trend to minimalizacja grubości ramki monitorów wielkoformatowych, wykorzystywanych do budowy tzw. ścian wideo (ang.: *video walls*). Są to modele serii 20 – NEC MultiSync LCD4020 (40-calowy) i MultiSync LCD 4620 (46-calowy).

Tą serią monitorów LCD z pewnością zainteresują się osoby, odpowiedzialne za wyposażanie centrów kontrolnych. Monitory te są zaprojektowane tak, aby działały bezawaryjnie przez długi czas. Mają wbudowane czujniki ciepła, nieustannie monitorujące wewnętrzną temperaturę ekranu. W przypadku przekroczenia maksymalnej, określonej przez użytkownika wartości zostają wykorzystane różne środki zapobiegające przegrzaniu, co gwarantuje nieprzerwane działanie. Osiągnięta w ten sposób niezawodność i długi czas eksploatacji, przekładają się na niski TCO (ang.: *Total Cost of Ownership* – całkowity koszt posiadania).

Monitory z tej serii mogą pracować w zastosowaniach wymagających podwyższonej szczelności – w obudowach o określonych klasach szczelności IP.

Kolejną innowacją jest zabezpieczenie antykradzieżowe. Nie pozwala ono na włączenie ekranu, dopóki nie zostanie wprowadzony czterocyfrowy kod PIN. Użytkownicy poszukujący elastycznych rozwiązań mają do dyspozycji wiele opcji rozszerzeń i złącz (np. wejście CAT 5, umożliwiające podłączenie do źródła sygnału przez skrętkę kategorii 5.

Adam Bułaciński

Spectra IV SE

Od ponad 10 lat zintegrowane kamery **Spectra** stanowią wzorzec, z którym porównywane są inne produkty. Spectra może być instalowana niemal w każdym środowisku ze względu na swoją niezawodność, wydajność oraz modułowość konstrukcji. Ustawienia dotyczące danej lokalizacji są przechowywane w nieulotnej pamięci w obudowie kamery. Dzięki temu dane wprowadzone podczas programowania pozostają niezmienione pomimo wielokrotnej wymiany głowicy. Spectra IV SE oferuje doskonałą optykę o rozdzielczości 540 TVL, obiektyw z 35-krotnym optycznym i 12-krotnym cyfrowym zoomem oraz zdolność do wytworzenia obrazów nawet przy bardzo słabym oświetleniu 0,00014 luksów. Inne jej zalety to m.in. elektroniczna stabilizacja obrazu, detekcja ruchu, 128-krotny zakres dynamiki.

Bezp. inf. Pelco

Nowy zamek w ofercie Dom Polska

Po raz kolejny firma Dom Polska wprowadza na rynek nowy produkt – zamek nawierzchniowy DOM 3050, przeznaczony do zamykania okien i drzwi. Dzięki specjalnej konstrukcji rygli może być stosowany zarówno do skrzydeł uchylnych jak i przesuwnych. W komplecie z zamkiem oferowane są podkładki montażowe, które zapewniają poprawny montaż w większości okien drewnianych, PVC, aluminiowych i stalowych dostępnych na rynku. Zamki Dom 3050 występują w kolorze białym lub brązowym. Posiadają certyfikat VdS.

Bezp. inf. Dom Polska

Bezprzewodowa wyspa

W 2008 roku Japonia planuje stworzyć na jednej ze swoich wysp obszar zaawansowanej technologii bezprzewodowej. W celu rozwoju tego programu rząd japoński będzie współpracował z producentami elektroniki, dostawcami usług telekomunikacyjnych, producentami samochodów i innymi zaawansowanymi technologicznie firmami.

Czujniki umieszczone na wyspie będą monitorować ruch drogowy. Pozwolą także szpitalom kontrolować zdrowie mieszkających w okolicy osób starszych. Zamiast identyfikatorów RFID, wykorzystujących do pracy częstotliwość radiową, zostaną użyte podobnie działające znaczniki IC bazujące na obwodach scalonych. Znaczniki IC są niewielkimi komputerowymi chipami z antenami.

Bezprzewodowa strefa będzie prawdopodobnie skonstruowana na Hokkaido lub Okinawie, ze względu na potrzebę minimalizacji zakłóceń.

Źródło: Daily Tech

Kluczowa naklejka

Osoby nerwowo szukające po kieszeniach karty, umożliwiającej wejście do biura, nie są widokiem niezwykłym. W końcu stale nosimy przy sobie jeszcze klucze do mieszkania, kluczyki do samochodu, telefon komórkowy, portfel, gazetę. Niektórzy noszą również etui na okulary, organizer, książkę, teczkę. W sumie – sporo tego. I jak tu się nie pogubić? Z pomocą przyszli nam specjaliści z koreańsko-amerykańskiej firmy **IDTECK**, którzy zaprojektowali breloki na klucze i naklejki na telefony komórkowe, pełniące funkcję kart zbliżeniowych.

Karty zbliżeniowe, za pomocą których dostajemy się do biura, nie są może ciężkie, ale znalezienie ich rano często graniczy z cudem. A przecież życie można sobie znacznie uprościć.

– *Breloki IDK 50 czy naklejki zbliżeniowe IMC 125 (czyli tagi) są ciekawym gadżetem ułatwiającym życie* – mówi **Radosław Majkowski**, dyrektor techniczny firmy **IPP**.

– *Breloki firmy IDTECK na pierwszy rzut oka nie różnią się od zwykłych produktów tego rodzaju, a naklejki mają wielkość zbliżoną do monety. Pomimo mniejszych gabarytów tagi te w niczym jednak nie ustępują tradycyjnym kartom zbliżeniowym – mają te same możliwości, są za to dużo bardziej poręczne od nich. Mamy też pewność, że o ile nie zgubiliśmy kluczy czy telefonu, z całą pewnością wejdziemy do biura.*

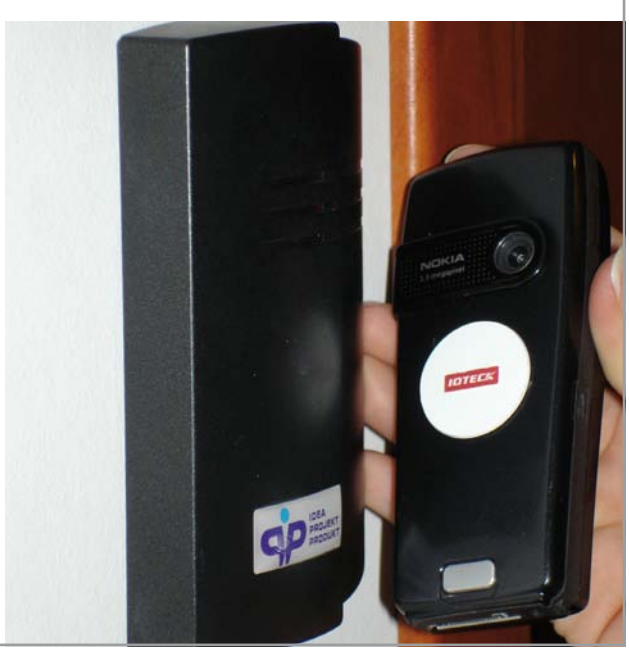
Tagi IDK 50 czy IMC 125 działają w paśmie 125 kHz i bez obaw można je stosować zamiennie do kart pasywnych. Pasują do większości czytników kontroli dostępu i mają też, dla określonego modelu czytnika, ten sam zasięg co karty zbliżeniowe – zwykle do 15 cm.

– *Istnieją także tagi w formie breloków i naklejek, w których można także zapisać informacje. Produkty te mogą być używane zarówno z tradycyjnymi czytnikami, jak i z czytnikami biometrycznymi* – dodaje Radosław Majkowski. – *Wówczas mogą mieć różne zastosowania, np. jako karta studencka, na której można zapisywać oceny lub wypożyczone z biblioteki książki, albo jako karta miejska, w której można zapisać wartość kwoty biletu okresowego, stan licznika itp.*

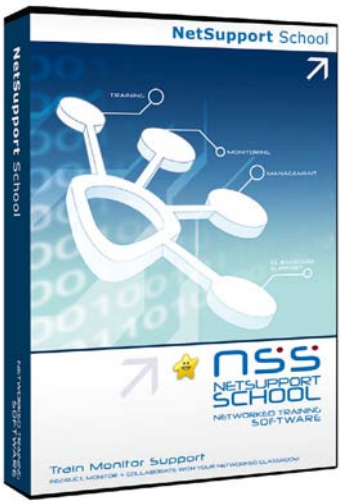
Powyższe tagi są zgodne z technologią Mifare i działają na częstotliwości 13,56 MHz.

Bezp. inf. T4B

Grupa T4B jest firmą z kapitałem polskim, powstałą w 2003 r. W jej skład wchodzą trzy podmioty: **T4B**, **IPP** oraz **TT Serwis**. Grupa T4B ściśle współpracuje z zagranicznymi firmami, takimi jak **IDTECK** czy **TAC**.



Nowa wersja programu NetSupport School



Oprogramowanie do monitorowania i zarządzania pracownią komputerową zapewnia nauczycielom jeszcze lepszą współpracę z uczniami i nadzór nad nimi.

Londyn, Wielka Brytania, 21 maja 2007: **NetSupport**, producent oprogramowania do zarządzania pracownią komputerową, ogłasza światową premierę nowej wersji programu **NetSupport School 9**.

Warszawa, 18 czerwca 2007: dostępna jest polska wersja NetSupport School 9.

Od 12 lat NetSupport School jest przodującym rozwiązaniem wspomagającym nauczanie i monitorowanie, pozwalającym nauczycielowi prowadzić podgląd ekranów uczniów oraz pokazywać im zawartość swojego ekranu. W ubiegłych latach dodano moduł kontroli użytkowania Internetu i aplikacji, egzaminowania oraz obsługę sieci bezprzewodowych, co umożliwiło dostosowanie programu do zmieniającego się kształtu zinformatyzowanej pracowni.

Wersja 9 idzie jeszcze dalej, dostarczając wielu dodatkowych, innowacyjnych funkcji, które usprawniają monitorowanie uczniów, redukują koszty użytkowania infrastruktury informatycznej oraz jeszcze bardziej zwiększają bezpieczeństwo uczniów i ich danych.

NetSupport School staje się pierwszym produktem w swej klasie, który standardowo zawiera moduł zarządzania drukarkami w pracowni, zapewniając narzędzia niezbędne do obniżenia kosztów druku.

NetSupport School to pierwszy produkt do zarządzania pracownią komputerową, zawierający funkcję monitorowania klawiatur w czasie rzeczywistym. Celem tego potężnego narzędzia jest podgląd aktywności studentów w czasie zajęć. Nauczyciel może sprawdzić nie tylko, czy wszyscy uczniowie używają edytora tekstów, ale także, czy piszą na temat.

Co więcej, NetSupport School również jako pierwszy oferuje monitorowanie komunikatorów internetowych w czasie rzeczywistym. Nauczyciel może zobaczyć, kiedy uczniowie logują się, wylogowują, rozpoczynają czat przy użyciu najpopularniejszych na świecie komunikatorów. Nauczyciel może również zamknąć sesję, na przykład, gdy uczeń przekazuje informacje o aktualnym teście kolegom.

NetSupport School zapewnia, również standardowo, proste i przejrzyste mechanizmy zabezpieczeń stacji uczniowskich. Jednym kliknięciem nauczyciel jest w stanie uniemożliwić uczniom dostęp lub kopiowanie danych do/z dysków USB oraz CD/DVD. W dużych pracowniach nauczyciel może również włączyć lub wyłączyć dźwięk w komputerach.

Najnowsza wersja NetSupport School posiada innowacyjną i unikatową funkcję Safe Search, automatycznie nakładającą filtr zawartości na rezultaty zwracane przez wyszukiwarkę internetową, niezależnie od osobistych ustawień użytkowników. Funkcja ta obsługuje istniejący w NetSupport School moduł kontroli Internetu i użycie list witryn dozwolonych i zabronionych, ograniczających uczniom swobodę poruszania się w Internecie. Mechanizm ten działa również w przypadku, gdy nauczyciel prowadzi prezentację. Zapobiega to sytuacji, w której przypadkowo na komputerze nauczyciela mogłaby zostać otwarta nieodpowiednia witryna w chwili, gdy jego ekran jest widoczny na komputerach uczniów.

Program zawiera też Pasek narzędzi studenta, informujący w czasie rzeczywistym o działaniach nauczyciela, monitorujący stan każdego ze składników programu, dostępność drukarek oraz wyświetlający listę aplikacji i stron internetowych, które w danej chwili uczeń może otwierać.

Nawet Kreator i Odtwarzacz egzaminów, uznawane za najlepsze rozwiązania tego typu, zostały ulepszone i wyposażone w nowy interfejs użytkownika, upraszczający zarządzanie zawartością i materiałami źródłowymi, oraz szybszy odtwarzacz pytań dla studentów. Najciekawszą nowością jest forum dostępne bezpłatnie dla wszystkich użytkowników NetSupport School. Nauczyciele mogą podzielić się na nim wiedzą, wymienić materiałami itp.

Na koniec jeszcze jedna bardzo istotna informacja. Obydwa moduły: Nauczyciel i Student, standardowo obsługują system Windows Vista. Obsługa sieci przewodowych i bezprzewodowych została znacznie rozszerzona, a nowy lokalizator uczniów wspomaga pracę w sieciach rozproszonych.

Wersja 9 programu NetSupport School to największa pojedyncza aktualizacja programu od jego premiery w roku 1995. Rozszerza ona możliwości zarządzania niezbędne nauczycielom w stale zmieniającym się środowisku skomputeryzowanych pracowni, czyniąc jeszcze bardziej efektywnymi narzędzia edukacyjne, prezentacyjne i egzaminacyjne produktu.

Darmowa, 30-dniowa wersja testowa programu dla 40 użytkowników jest dostępna na stronie internetowej *http://www.netsupportschool.com.*

NetSupport School został wyróżniony nagrodą Technology&Learning Legacy Award of Excellence 2006, przyznaną za produkt najwyższej jakości w swej klasie, wyraźnie przewyższający inne dostępne na rynku rozwiązania, oraz nagrodą BESSIE dla najlepszych programów edukacyjnych – Best Educational Software Awards 2007, przyznawaną przez ComputED.

Dystrybucją produktów NetSupport w Polsce zajmuje się firma ALWO.

Bezp. inf. ALWO

IFSEC 2007

Międzynarodowe targi zabezpieczeń IFSEC'2007 odbyły się w dniach 21–24 maja tradycyjnie w Birmingham, drugim pod względem wielkości mieście w Wielkiej Brytanii, na terenie NEC (Narodowego Centrum Wystawienniczego). W tym jednym z najlepiej zorganizowanych centrów wystawowych na świecie swoje produkty związane z branżą zabezpieczeń prezentowało ponad 700 wystawców z całego świata.

Najwięcej prezentowano urządzeń służących do obserwacji, rejestracji oraz odtwarzania obrazów wizyjnych. Trend ten można zaobserwować od kilku lat. Jedne z największych stoisk w tym segmencie miały firmy Pelco oraz azjatycki Samsung. Swoje produkty pokazali oczywiście nie tylko potentaci w tej branży, ale również wiele mniejszych firm, zwłaszcza z dalekiej Azji, które od lat traktują targi jako świetną okazję do znalezienia nowych dystrybutorów na rynku europejskim.

Coraz szersze kręgi zatacza technologia IP i asortyment urządzeń, w których ma zastosowanie (przede wszystkim w systemach telewizji dozorowej) jest coraz większy. Wielu europejskich, amerykańskich czy też japońskich wystawców pokazywało oprogramowanie służące do śledzenia obiektów ruchomych lub wyposażenie centrów monitoringu.

Producenci systemów alarmowych antywłamaniowych skupili się tym razem głównie na walorach estetycznych, przedstawiając całą gamę kolorów klawiatur. Dominującym kolorem podświetlenia stał się niebieski.

Swoje produkty przedstawili także producenci systemów sygnalizacji pożarowej.

Kontrola dostępu wyraźnie zmierza w stronę rozwiązań biometrycznych, zwłaszcza wykorzystujących analizę odcisku palca. Tutaj największy wybór produktów oferowały firmy koreańskie, obecne były również japońskie (Hitachi, JVC). Z firm europejskich bardzo zaawansowane rozwiązania tego rodzaju pokazała francuska firma Sagem. Najczęstsze rozwiązania to urządzenia mieszczące w jednej obudowie sensor biometryczny, czytnik kart zbliżeniowych wyświetlacz LCD (często kolorowy) oraz klawiaturę kodową do celów KD i RCP.

Organizatorzy targów duży nacisk położyli na uświadamianie ludziom czyhających na nich zagrożeń. Dlatego zorganizowano bezpłatne seminaria poświęcone elektronicznemu bezpieczeństwu.

Warto również nadmienić, że na targach swoje stoiska posiadały polskie firmy, takie jak **Satel, Roger** oraz **Kamet**.

Imprezą towarzyszącą targom było ogłoszenie laureatów nagród za innowacje w dziedzinie zabezpieczeń. Uroczystość odbyła się w hotelu Hilton Metropole w Birmingham. Wśród jurorów znaleźli się przedstawiciele Stowarzyszenia Brytyjskiego Przemysłu Zabezpieczeń (BSIA) i wydziału ds. rozwoju naukowego brytyjskiej policji. James Blue, dyrektor IFSEC, powiedział: „Gdy obserwuje się zmiany, które zaszły w ciągu ostatnich 12 miesięcy w brytyjskim przemyśle zabezpieczeń, widać, że poprzeczka podnosi się i wyznaczane są wysokie standardy do osiągnięcia. Te nagrody to idealna okazja, aby docenić firmy, które spełniają takie wymagania".

Przyznano następujące nagrody:

- „Najlepsza z najlepszych" (ang.: *Best of the Best Award*) – włoskiej firmie Cieffe za produkt Nettuno Mega PX – pierwszą w świecie kamerę CCTV, w której połączono megapikselową rozdzielczość z kompresją MPEG4, co pozwala na uniknięcie ograniczeń, występujących w przypadku kompresji JPEG;
- „Najlepszy nowy produkt" – w pięciu kategoriach:
  - kontrola dostępu – firmie Panasonic System Solutions Europe za czytnik biometryczny BM-ET 200 – kamerę do tęczówki oka z układem dwóch luster, ułatwiającym uzyskanie właściwego położenia obu oczu do identyfikacji, trwającej zaledwie ok. 0,3 sekundy;
  - CCTV – ponownie Cieffe za Nettuno Mega PX;
  - IP Security – jednemu z brytyjskich liderów monitoringu obiektów stałych i ruchomych – firmie BT Redcare, za system monitorowania alarmów RedCare Assure, wykorzystujący dwudrożną transmisję IP do przesyłania sygnałów alarmowych oraz podglądu wideo;
  - ochrona fizyczna – brytyjskiej firmie Concept Smoke Screen za przenośny system ochrony dymnej Rapid Deploy;
  - system sygnalizacji włamania – amerykańskiej firmie Ultra Vision Security Systems za detektor ruchu Ultra Sensor do zastosowań wewnętrznych i zewnętrznych, wykorzystujący znaną z zastosowań w badaniach geofizycznych szerokopasmową technologię UWB (ang.: *ultra wide band*) do detekcji intruzów w promieniu do ok. 7,5 m od miejsca ukrycia nadajnika/odbiornika Ultra Sensor i umożliwiającą uzyskanie nie tylko informacji o detekcji ruchu, ale także o masie, prędkości i odległości od intruza;
- „Najlepszy nowy projekt lub instalacja" – ntl:Telewest Business wraz z Controlware Communications za pionierski projekt oraz implementację jednej z większych instalacji IP CCTV w Europie (wartej ponad 1,3 mln GBP), podnoszącej bezpieczeństwo w liczącym ponad 320 tys. mieszkańców hrabstwie North Lanarkshire w centralnej Szkocji;
- nagrodę „ACPO za wykorzystanie technologii do poprawy bezpieczeństwa publicznego" (ACPO – stowarzyszenie oficerów policji Anglii, Walii i Irlandii Płn.) – brytyjskiej firmie Connexion2 za SoloProtect, czyli usługę, zapewniającą ochronę osobistą z wykorzystaniem noszonego jako identyfikator ze zdjęciem urządzenia Identicom – miniaturowego nadajnika GSM z przyciskiem napadowym;
- nagrodę lidera branży security (ang.: *Security Industry Leadership Award*) – uzyskał ją John Saunders OBE;
- nagrodę „Osobowość roku branży security" (ang.: *Security Industry Personality Of The Year*), której laureatem został Ian Nisbet z G4S Cash Services.

Następne targi IFSEC odbędą się na terenie NEC w dniach **12-15 maja 2008 r.** Organizatorzy już teraz zapewniają, że będą one większe i lepsze niż kiedykolwiek dotychczas.

Redakcja

WARSZTATY w Borach Tucholskich

Zakład Urządzeń Dozymetrycznych **Polon-Alfa** zorganizował w tym roku piętnaste już, a więc jubileuszowe Ogólnopolskie Warsztaty – Systemy Sygnalizacji Pożarowej Zacisze 2007. W dniach 31.05-02.06 2007, na zaproszenie organizatorów, których reprezentował prezes zarządu Jerzy Karczewski, do Ośrodka Doskonalenia Kadr Służby Więziennej w Suchej przybyli wybitni specjaliści z Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej z Józefowa (Eugeniusz Wojciech Roguski – dyrektor naczelny CNBOP, Janusz Sawicki, Jerzy Ciszewski, Rafał Turkiewicz), ze Szkoły Głównej Służby Pożarniczej (Waldemar Wnęk), komendant PSP województwa kujawsko-pomorskiego – Tomasz Leszczyński, Krzysztof Dąbrowski – prezes stołecznego oddziału SITP reprezentujący prezesa SITP Bronisława Skaźnika, dyrektor Izby Rzeczoznawców SITP – Ryszard Małolepszy, przedstawiciel „Polalarmu" – Alojzy Pawelczak, komendant miejski PSP w Bydgoszczy – Wojciech Gmurczyk, komendant powiatowy PSP w Nakle n. Notecią, a także przedstawiciele firm projektowo-instalacyjnych, które zajmują się również konserwacją systemów sygnalizacji pożarowej. W warsztatach uczestniczyli także zagraniczni partnerzy firmy Polon-Alfa: Bogdan Kupowicz – BK Company Ukraina, Giedrius Taraskievicius – LEVORISKIS Litwa, Stieła Czawdarowa – EVRO-TUR Bułgaria.

Grzechem byłoby nie opisać choćby w kilku zdaniach miejsca, do którego raz do roku, od kilkunastu już lat, przyjeżdżają ludzie z całej Polski, aby z dala od zgiełku miasta, od głównych dróg, polityki, zbędnych emocji pogłębić wiedzę oraz wymienić doświadczenia z zakresu instalowania i projektowania systemów sygnalizacji pożarowej.

Ośrodek Doskonalenia Kadr SW Zacisze k/Klonowa, w którym od 1993 roku organizowane są warsztaty, znajduje się na półwyspie otoczonym wodami Zalewu Koronowskiego w sercu Borów Tucholskich. Na obszarze regionu przeważa bór sosnowy. Zachowały się jednak również szczątki dawnej Puszczy Pomorskiej, gdzie spotkać można polodowcowe relikty, takie jak brzoza karłowata, cis pospolity, brekinia. Na obszarze regionu znajduje się ponad 900 jezior. Są tu także sztuczne zbiorniki, do których zalicza się między innymi Zalew Koronowski, oraz malownicze rzeki, z których największe, Brda i Wda, uchodzą za jedne z piękniejszych tras spływów kajakowych.

Wybór miejsca okazał się strzałem w dziesiątkę. Komfortowe warunki doskonale przystosowanego do organizacji tego typu imprez ośrodka oraz diametralnie różny od wielkomiejskiego krajobraz za oknem sprzyjały chłonięciu wiedzy serwowanej przez wybitnych specjalistów – znawców tematu.

Uroczystego rozpoczęcia warsztatów dokonał prezes zarządu ZUD Polon-Alfa, Jerzy Karczewski.

W warsztatach wzięło udział 160 osób. Zainteresowanie szkoleniem przerosło najśmielsze oczekiwania, a w związku z ograniczoną liczbą miejsc (brak dostatecznie dużej bazy noclegowej) nie można było przyjąć wszystkich chętnych.

Nie sposób nie zauważyć, jak wielki postęp dokonał się w dziedzinie techniki w ciągu ostatnich lat. Mimo to problemy związane z wykonawstwem i utrzymaniem instalacji w sprawności pozostają wciąż te same – błędy projektowe, źle wykonane i nie konserwowane instalacje. Jak twierdzą specjaliści, przyczyną tego stanu jest między innymi nieprecyzyjność lub całkowity brak odpowiednich przepisów, a także brak obowiązku certyfikacji firm świadczących usługi projektowe, instalatorskie i serwisowe. Dlatego tegoroczne warsztaty poświęcone były przede wszystkim zagadnieniom wykonywania instalacji, organizacji procesów instalowania, odbioru oraz utrzymania instalacji.

Przygotowany program był napięty i wypełniony po brzegi różnego typu zajęciami. Wygłoszono w sumie dziesięć referatów – pierwszego dnia – trzy:

1. *Nowości wdrożone w Polon-Alfa (Przegląd czujek wielodetektorowych produkowanych w Polon-Alfa)* – dyr. Lech Światły

2. *Błędy popełniane przez projektantów instalacji sygnalizacji pożarowej i automatyki pożarniczej* – Mariusz Sobecki, SITP, Oddział Katowice, Koło Legnica

3. *Wybrane problemy projektowania i instalowania systemów sygnalizacji pożarowej* – Jerzy Ciszewski, CNBOP, Józefów

Ukoronowaniem pierwszego dnia była uroczysta kolacja, podczas której za szczególne zasługi dla firmy nagrodzeni zostali Złotymi Odznakami 50-lecia Polon-Alfa Jerzy Ciszewski i Janusz Sawicki z CNBOP oraz Stefan Świtula – dyrektor biura handlowego Polon-Alfa. Pożegnano również przechodzącego na emeryturę wybitnego specjalistę w dziedzinie zabezpieczeń, a także normalizacji obejmującej zakres systemów sygnalizacji pożarowej – Władysława Markowskiego (w tym roku był po raz 12 moderatorem warsztatów).

W rytm gorącej muzyki goście bawili się do białego rana, dając dowód na to, że to właśnie w Zaciszu odbywają się jedne z najlepszych branżowych imprez.

Drugiego dnia wygłoszono kolejne siedem referatów:

1. *Prawne i praktyczne aspekty odbiorów instalacji sygnalizacji pożarowej* – Adam Somerlik, SITP, Oddział Katowice.

2. *Zasady prowadzenia przeglądów i obsługi technicznej instalacji urządzeń przeciwpożarowych* – Janusz Sawicki, CNBOP.

3. *Wpływ osłon przeciwwietrznych na czas zadziałania systemów sygnalizacji pożarowej* – Waldemar Wnęk, SGSP.

4. *Systemy podtrzymania funkcji OBO-Bettermann* – Tomasz Marszałek.

5. *Technologie połączeń oraz asortyment WAGO dla instalatorów* – Michał Grabowski, WAGO ELWAG.

6. *Systemy sieciowe w sygnalizacji pożarowej* – Rafał Turkiewicz, CNBOP.

7. *Kable sensoryczne firmy LISTEC jako liniowe czujki ciepła* – Arkadiusz Waligóra, CREATIO Business Development.

Atrakcją drugiego dnia był niewątpliwie rejs statkiem pasażerskim, w tym dniu pod banderą Polon-Alfa. Aby było jeszcze przyjemniej, kapitan serwował kawę po kapitańsku.

Wieczorem zorganizowano konkurs „Złap byka za rogi" – wszyscy odważni, a było ich wielu, stanęło w szranki z szalejącym, na szczęście tylko elektrycznym, bykiem. Należy wspomnieć, że panie dawały sobie świetnie radę – przy olbrzymim dopingu uplasowały się na bardzo wysokich miejscach.

Na zakończenie wszyscy wzięli udział w ognisku. Był to również czas dzielenia się wrażeniami po zakończonych warsztatach i zdobytym doświadczeniem. Śpiewom i rozmowom nie było końca. Najwytrwalsi dotrwali do wczesnych godzin rannych.

Trzeciego dnia był już tylko relaks i ładowanie akumulatorów przed powrotem do codziennych obowiązków. Odbyła się wycieczka do największego w Europie rezerwatu cisów w Wierzchlesie, nazywanego skarbem Borów Tucholskich (nazywając rezerwat cisów imieniem Leona Wyczółkowskiego oddano hołd pamięci artysty, który spędził w nim w okresie międzywojennym wiele czasu, znajdując tu spokój i natchnienie). W tym malowniczym uroczysku, które ochrzcił mianem „świętego gaju", wykonał w sumie ponad 100 prac. Jego dzieło przedstawiające najstarszy w rezerwacie cis „Chrobry" (obwód 232 cm, wiek około 600 lat) uzyskało na wystawie w Wenecji I nagrodę. Niektóre prace można do dzisiaj podziwiać w Muzeum Okręgowym im. Leona Wyczółkowskiego w Bydgoszczy.

Jeżeli ktoś lubi atmosferę tajemniczości, zadumy, lubi poczuć tchnienie minionych wieków, to namawiam do odwiedzenia tego prawdziwie bajkowego lasu.

Dla wszystkich uczestników organizatorzy przygotowali komplet materiałów informacyjnych, w skład których weszła m.in. broszura zawierająca referaty poświęcone tematowi wiodącemu warsztatów.

W kuluarach warsztatów nieustannie toczyły się rozmowy, nawiązywano nowe kontakty, spotykano dawno nie widzianych znajomych. Można było również obejrzeć prezentacje firm OBO BETTERMANN, IP&S (Industrial Products & Services), WAGO ELWAG, Polon-Alfa.

Podczas warsztatów firma OBO BETTERMANN zaprezentowała szereg praktycznych systemów – prostych w montażu i sprawdzonych na zgodność z wymaganiami normy DIN 4102-12 w zakresie prowadzenia przewodów i kabli o odporności ogniowej PH90. Omówiono zastosowanie koryt kablowych, drabin poziomych i pionowych oraz uchwytów i obejm wraz z certyfikowanymi kotwami. Podano informacje techniczne na temat produktów OBO stosowanych w systemach ochrony przeciwpożarowej.

Firma IP&S przedstawiła adresowalny system Eagle Quantum Premier. Jest on produkowany przez Detector Electronics z USA, której firma IP&S jest autoryzowanym dystrybutorem. System ten służy do wykrywania niebezpiecznych stanów w instalacjach przemysłowych, w strefach zagrożonych wybuchem oraz do sterowania urządzeniami infrastruktury bezpieczeństwa (systemy sygnalizacji, gaszenia, wentylacji, blokad awaryjnych, wizualizacji itp.). Do systemu można wprowadzić dowolne sygnały z czujek pożarowych, gazowych, ciśnienia, temperatury, sygnalizatorów przekroczenia zadanych parametrów, wyłączników krańcowych itp. Moduły wejściowe systemu akceptują sygnały zarówno analogowe, jak i dwustanowe. Centrala systemu umożliwia zaprogramowanie dowolnej logiki sterowania sygnałami wyjściowymi. Centrala i główne elementy liniowe są certyfikowane przez TÜV i przeznaczone do stosowania w systemach o poziomie nienaruszalności bezpieczeństwa SIL-2.

Uczestnicy zapewnili, że przyjadą tu znów za rok.

Teresa Karczmarzyk

Więcej zdjęć na naszej stronie internetowej **http://www.zabezpieczenia.com.pl** w dziale Fotoreportaże.

Schrack Seconet Polska

Ogólnopolskie Szkolenie Projektowe 2007

RELACJA

Kolejne **Ogólnopolskie Szkolenie Projektowe** firmy **Schrack Seconet Polska** odbyło się 20 czerwca 2007 roku w Warszawie. Uczestniczyło w nim ok. 200 osób – głównie projektantów SSP (systemów sygnalizacji pożarowej). W gronie prelegentów znalazło się dwóch gości specjalnych z CNBOP (Janusz Sawicki i Jerzy Ciszewski), przedstawiciel firmy Ambient System, znanej dawniej pod nazwą Mercor System (Bogusław Adamczyk), oraz pracownicy firmy Schrack Seconet Polska pod przewodnictwem prezesa zarządu Grzegorza Ćwieka – Krzysztof Kunecki i Paweł Tomaszewski.

Na wstępie Grzegorz Ćwiek poinformował o programie szkolenia oraz o ostatnich zmianach organizacyjnych w firmie Schrack Seconet Polska, w wyniku których objął on od kwietnia br. stanowisko prezesa zarządu i dyrektora generalnego. Zastąpił na tym stanowisku Piotra Pajora, który piastował je od siedmiu lat. Grzegorz Ćwiek jeszcze wielokrotnie zabierał głos – w swojej sesji tematycznej, a także zapowiadając, a następnie komentując wystąpienia innych prelegentów i podsumowując szkolenie w wystąpieniu końcowym. Przedstawił także wyniki ogłoszonego jesienią 2006 roku konkursu dla projektantów SSP.

W konkursie tym przyznano „za wysoką jakość i poprawność projektów SSP opartych na urządzeniach Schrack Seconet w r. 2006/2007" dwie równorzędne nagrody oraz wyróżnienie. Laureatami nagród (wizyta w siedzibie głównej firmy Schrack Seconet) zostali:

- **Marek Achinger**, który w 2006 roku zaprojektował kilka systemów SSP o istotnym znaczeniu, m.in. za projekt do najbardziej skomplikowanego pod tym względem, 194-metrowego biurowca „Rondo 1" w Warszawie,
- **Wojciech Pobłocki** – autor kilkunastu projektów, w tym systemu sieciowego BMZ Integral w jednym z największych zakładów przemysłowych w Polsce.

Wyróżnienie i prezent od firmy otrzymał Grzegorz Liber. Wszystkich trzech laureatów uhonorowano także dyplomami uznania. Jednocześnie został ogłoszony nowy konkurs, dotyczący projektów SSP realizowanych z wykorzystaniem rozwiązań Schrack Seconet.

Podczas szkolenia poruszono i podsumowano niżej wymienione zagadnienia:

1. Scenariusz rozwoju zdarzeń na wypadek pożaru – odpowiedzialność projektanta, zasady tworzenia. Wpływ przyjętego scenariusza rozwoju zdarzeń na dobór urządzeń wykonawczych systemu przeciwpożarowego (Janusz Sawicki, CNBOP).

Zasady tworzenia systemów przeciwpożarowych (systemów sygnalizacji pożarowej, stałych urządzeń gaśniczych, dźwiękowych systemów ostrzegania, wydzieleń pożarowych) wynikają z przyjętych scenariuszy pożaru. To trudne zadanie, jakim jest opracowanie scenariuszy pożarowych, należy do: rzeczoznawców ds. zabezpieczeń przeciwpożarowych z uprawnieniami Państwowej Straży Pożarnej, ekspertów z towarzystw ubezpieczeniowych i przedstawicieli Głównego Urzędu Nadzoru Budowlanego (o czym nie należy zapominać).

2. Najnowsze urządzenia Schrack Seconet wprowadzane do sprzedaży w roku 2007 (Krzysztof Kunecki, Schrack Seconet Polska):

- centrala sygnalizacji pożarowej Integral Evolution,
- ewolucja central sygnalizacji pożarowej Schrack Seconet,
- interaktywna czujka multisensorowa CUBUS MTD 533.

W przedstawionej ewolucji central SSP firmy Schrack Seconet, sięgającej 1980 roku, widać wpływ rozwoju technologii na właściwości coraz to nowych urządzeń. Ważną cechą nowych urządzeń jest ich kompatybilność z dotychczas produkowanymi. Nowa centrala Integral Evolution (platforma B5), która pojawi się w III kwartale 2007 roku, będzie kompatybilna z peryferiami obecnie sprzedawanego modelu Integral (platforma B3). Karty platformy B3 będą mogły pracować z Integral Evolution, a nowe karty platformy B5 – w obecnie dostępnych rozwiązaniach. Kompatybilność jest także zachowana w nowej generacji czujek inteligentnych Cubus MTD 533, które będą stosowane z używanymi obecnie gniazdami USB 501. Ten nowy model czujki wielosensorowej zastąpi dotychczas stosowane czujki optyczne DMD2000 i temperaturowe OSD2000, gdyż może być stosowany zarówno jako czujka temperatury, dymu (ale, co warto podkreślić, z dodatkową analizą temperatury), jak i jako czujka dualna.

3. Aktualny stan certyfikacji urządzeń Schrack Seconet w Polsce (Krzysztof Kunecki, Schrack Seconet Polska).

W celu uzyskania aktualnej informacji na ten temat najlepiej zwrócić się do firmy Schrack Seconet Polska.

4. Nowa oferta Schrack Seconet – podsumowanie, nowe zasady dystrybucji materiałów informacyjnych (Grzegorz Ćwiek, Schrack Seconet Polska).

Nowa oferta to także nowe ceny. Firma Schrack Seconet wprowadza nowości z reguły w cenach nie wyższych niż ceny sprzętu dotychczas oferowanego. Tak będzie i tym razem. Czujka Cubus MTD 533 będzie oferowana w cenie nie

wyższej niż obecnie obowiązująca dla czujki OSD 2000, a nowa centrala Integral Evolution będzie tańsza niż model Integral. W ciągu ostatnich dwóch lat nastąpiła obniżka cen produktów Schrack Seconet rzędu 2–5%, a od sierpnia br. do końca roku 2008 przewiduje się dalszą obniżkę cen o kolejne 2–5%. Nowe formy komunikacji z partnerami Schrack Seconet Polska to z kolei: zwiększenie roli poczty elektronicznej, nowa formuła strony internetowej (od września br.), przewidująca spersonalizowany dostęp do danych po zalogowaniu – z treścią zależną od własnych potrzeb i oczekiwań – i możliwość zgłaszania się w trybie on-line na organizowane przez firmę szkolenia i inne imprezy, nowa forma prezentacji dokumentacji – w postaci układanki, której elementy będą stopniowo rozświetlane, w miarę powstawania kolejnych elementów dokumentacji.

5. Przykłady zastosowania czujek wielodetektorowych w obiektach – wytyczne projektowania (Jerzy Ciszewski, CNBOP).

Podczas projektowania SSP należy uwzględniać zarówno zasięgi czujek, pamiętając o tym, że są one różne dla różnych trybów ich pracy, jak i wysokości zabezpieczanych pomieszczeń. Dlatego czujki temperaturowe, pracujące w zbyt wysokich pomieszczeniach, stają się nieskuteczne (czujka dualna dymu i ciepła w pomieszczeniu wyższym niż 8 m działa tylko jak czujka dymu). Oddzielnym zagadnieniem jest koincydencja działania czujek. Poglądy na ten temat ostatnio się zmieniają.

6. Sterowanie stałymi urządzeniami gaszenia – przegląd obowiązujących wytycznych – centrale dedykowane oraz centrale zintegrowane – organizacja pętli wykrywczych i sterujących – zasady stosowania (Jerzy Ciszewski, CNBOP).

Warto przeanalizować przedstawione w wystąpieniu przykłady nieprawidłowego zaprojektowania SSP, aby uniknąć podobnych błędów w swoich projektach. Nie wolno zapomnieć o możliwym wpływie zakłóceń elektromagnetycznych na działanie całego systemu (o czym wspominał autor referatu, omawiając m.in. przypadki z własnego doświadczenia).

7. Aktualne wytyczne w zakresie stosowania urządzeń Schrack Seconet (Krzysztof Kunecki, Schrack Seconet Polska):
– systemy sterowania gaszeniem – aktualności,
– rozwiązania specjalne.

Urządzenia Schrack Seconet w pełni umożliwiają sterowanie i nadzorowanie instalacji gaśniczych, nie tylko w zakresie czterech podstawowych funkcji systemów stałych urządzeń gaśniczych, ale i funkcji fakultatywnych (była o nich mowa w poprzednim referacie). Centrala BLZ/SLZ Integral C przy zastosowaniu specjalnej wersji obudowy, dodatkowych elementów systemu oraz tablicy wskazań z diodami LED – jako centrala sterująca dla jednej strefy gaszenia, a system BLZ/SLZ Integral, zgodnie z wymaganiami norm i wytycznych EN12094-1, jak również VdS2469 – sterowanie oraz nadzorowanie w więcej niż jednej strefie gaszenia (certyfikacja CNBOP – w trakcie).

8. Współpraca systemów DSO i SAP. Podstawowe zasady konfiguracji systemów sieciowych DSO (Bogusław Adamczyk, Ambient System).

Dźwiękowe systemy ostrzegawcze muszą spełniać wymogi normy PN-EN 60849: 2001, której punkt 5.5. dotyczy wymagań, związanych ze współpracą z SSP. Jedno z wymagań nie zawsze jest traktowane jako priorytetowe, a dotyczy tego, że DSO musi być zdolny do wysłania do SSP co najmniej jednego sygnału: „DSO uszkodzony". Firma Ambient System jest dystrybutorem systemu rozgłaszania publicznego mcr Venas, który spełnia wszystkie wymagania, dotyczące pracy DSO w warunkach normalnych, jak i podczas zagrożenia, przeznaczony do stosowania w obiektach o dowolnej funkcji użytkowej. Może być skonfigurowany zarówno do pracy w układzie sieciowym, jak i z wyniesionym mikrofonem strażaka, co potwierdza przyznanie certyfikatu CNBOP.

9. Najnowszy system komunikacji Visocall IP. Zastosowanie systemów komunikacji w obiektach komercyjnych (Paweł Tomaszewski, Schrack Seconet Polska).

W charakterze systemów przywoławczych są niekiedy stosowane w szpitalach i innych obiektach, w których są wymagane, systemy domofonowe. Są jednak przecież dostępne dedykowane systemy, służące do tych celó w, także nadające się do obiektów komercyjnych. Przykładem – praktycznie bezkonkurencyjnym na polskim rynku – jest nowa wersja systemu przywoławczego firmy Schrack Seconet – Visocall IP. Jest to rozwinięcie znanego od lat systemu Visocall MP2, przy czym komunikacja pomiędzy poszczególnymi elementami systemu odbywa się z wykorzystaniem sieci komputerowej. Takie rozwiązanie wyznacza nowy standard w cyfrowej komunikacji szpitalnej. Przy niewielkiej modyfikacji istniejącej infrastruktury można istotnie obniżyć koszty instalacji systemu przywoławczego, unikając prowadzenia dedykowanego okablowania – zarówno sygnałowego, jak i przeznaczonego do zasilania urządzeń. System spełnia normy niemieckie VDE0834 (normy polskie na temat tego typu systemów nie istnieją) i jest przewidziany do sprzedaży od I kwartału 2008 roku.

Adam Bułaciński

15 lat minęło

„Mam nadzieję, że za kolejne 15 lat spotkamy się w jeszcze większym gronie i wspólnie będziemy świętować naszą trzydziestkę" – takimi słowami zakończył przemówienie powitalne prezes **ela-compil**, **Norbert Bartkowiak**. 16 czerwca w Gospodzie Młyńskie Koło poznańska **firma obchodziła swoje 15-lecie**. Na zaproszonych gości czekały liczne atrakcje artystyczne i przygotowane specjalnie na tę okazję przysmaki szefa kuchni Gospody.

Wielu estetycznych i smakowych doznań dostarczył gościom pokaz barmański. Zdobywca tytułu wicemistrza świata prezentował zebranym swoje umiejętności i zapraszał ich do wspólnego przygotowywania smakowitych trunków. Uczeń Eugeniusza Dytki zaprezentował nie tylko swoje talenty barmańskie, ale także pirotechniczne walory napojów wyskokowych.

Podczas przemówienie prezesa, Norberta Bartkowiaka, kilku pracownikom zakręciła się łza w oku. Prezes przypominał wspólnie przepracowane lata, opowiedział firmowe anegdotki. Wystąpieniu towarzyszyły gratulacje i podziękowania ze strony gości: kontrahentów, współpracowników, klientów i samych pracowników.

Po wspólnej uroczystej kolacji nadszedł czas na dobrą zabawę. Prowadzący zapowiedział specjalnego gościa wieczoru – Ireneusza Krosnego. Spektakl złożony z kilku niepołączonych ze sobą fabularnie etiud ponownie doprowadził zebranych do płaczu – tym razem ze śmiechu. Ubrany jak zawsze na czarno i bez makijażu, mim odegrał swoje najlepsze scenki, takie jak: **Dyrygent, Chirurg, Miss Wieczorem, Bodyguard czy Z wizytą u szefa**.

Około godziny 22.00 nad jeziorem znajdującym się przy Młyńskim Kole rozległy się dźwięki utworu Vangelisa, który towarzyszył pokazowi sztucznych ogni..

Następnie, jeszcze pod wrażeniem pokazu, goście przeszli do sali, w której czekała na nich następna niespodzianka – kasyno. Przez kolejne godziny w Gospodzie rządziło koło fortuny. Ruletka, poker i Black Jack cieszyły się dużym powodzeniem. Nie było osoby, która nie chciałaby spróbować szczęścia.

Niesłabnącą popularnością cieszyło się karaoke. Okazało się, że pracownicy ela-compil są nie tylko specjalistami w dziedzinie zabezpieczeń. Drzemie w nich ukryty talent muzyczny. Zaproszeni klienci nie chcieli pozostać w tyle i dołączyli do solistów, tworząc bardzo ciekawe i zróżnicowane pod względem wokalnym, duety, tercety, a nawet kwartety.

Atmosfera zabawy i świętowania oraz pogodna aura sprzyjały długim rozmowom do późnych godzin nocnych.

Bezp. inf. elacompil

ela-compil – dostawca najnowszej generacji technologii BMS wspomagającej zarządzanie budynkiem. Opracowuje i dostarcza rozwiązania oparte na najnowszych osiągnięciach myśli technologicznej zarówno w zakresie oferty produktowej, jak i tworzonych koncepcji nowoczesnego i efektywnego zarządzania budynkiem oraz zapewnienia odpowiedniego poziomu bezpieczeństwa. Sztandarowym produktem w ofercie firmy jest System Zarządzania Budynkiem GEMOS, na który ela-compil posiada wyłączność w zakresie dystrybucji na terenie Polski.

System GEMOS pomaga w utrzymaniu budynków w wysokiej sprawności technicznej, funkcjonalnej, organizacyjnej i ekonomicznej. Dzięki kompleksowej integracji wszystkich systemów zainstalowanych w danym obiekcie zapewnia sprawne jego zarządzanie oraz wysoki poziom bezpieczeństwa obiektu (kompleksu obiektów) o różnorodnym przeznaczeniu: handlowym, biurowym, przemysłowym, sportowym itd.

Atutem systemu GEMOS jest jego neutralność względem producentów urządzeń, w które jest wyposażony obiekt. To zapewnia inwestorom i zarządcom nieruchomości możliwość wyboru z wielu produktów obecnych na rynku i sprawia, że system GEMOS może je integrować i nimi zarządzać. GEMOS może być instalowany zarówno w obiektach nowych, jak i w budynkach istniejących, wyposażonych w różne systemy, które nie były dotychczas integrowane.

GEMOS zarządza:
- systemami bezpieczeństwa, w skład których wchodzą:
  - systemy sygnalizacji pożaru
  - dźwiękowe systemy ostrzegawcze
  - systemy sygnalizacji włamania i napadu
  - systemy kontroli dostępu
  - systemy telewizji dozorowej
  - systemy wentylacji pożarowej
  - inne systemy automatyki pożarowej
- systemami automatyki budynkowej, do których należą:
  - systemy wentylacji i klimatyzacji
  - systemy sterowania windami
  - system zasilania
  - systemy oświetlenia ewakuacyjnego
  - systemy łączności wewnętrznej
  - systemy zarządzania kluczami

Satel - Inteligentne systemy alarmowe

Kładziemy duży nacisk na obsługę Klienta

Od 17 lat specjalizujemy się wyłącznie w produkcji urządzeń do systemów alarmowych. Nie tylko jakość samego produktu jest dla nas istotna. Dbamy, aby stała dostępność pełnej oferty, wsparcie techniczne i jakość obsługi wpłynęły na zadowolenie instalatorów i inwestorów indywidualnych z użytkowania naszych produktów.

- produkty SATEL dostępne są na terenie całego kraju w ponad 50 punktach dystrybucyjnych
- posiadamy kompletną ofertę urządzeń potrzebnych do realizacji dowolnego systemu alarmowego
- prowadzimy szkolenia, prezentacje i warsztaty, gdzie dzielimy się wiedzą, uczymy i rozmawiamy z naszymi Klientami, aby ciągle udoskonalać nasze produkty
- umożliwiamy dostęp do aktualnych informacji o firmie i produktach poprzez stronę www.satel.pl
- nasi specjaliści udzielają porad technicznych w zakresie instalowania i obsługi naszych produktów
- serwis znajdujący się w Gdańsku, umożliwia sprawne i skuteczne załatwienie ewentualnych reklamacji
- zapewniamy bezpośredni kontakt z naszymi Konsultantami handlowymi na terenie całego kraju

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

EIB
rozproszony system zarządzania budynkiem

W numerze 3. *Zabezpieczeń* rozpoczęliśmy cykl artykułów na temat Europejskiej Magistrali Instalacyjnej (ang.: *European Installation Bus*, EIB). Jest to technologia wykorzystywana najczęściej w zastosowaniach innych niż elektroniczne systemy bezpieczeństwa, głównie ze względu na jej otwarty charakter. Choć w wielu przypadkach nie gwarantuje wystarczającego stopnia zabezpieczenia przed nieautoryzowaną ingerencją, to jednak umożliwia także zarządzanie systemami, związanymi z ochroną życia i mienia w budynkach.

Część pierwsza artykułu pozwoliła PT Czytelnikowi na usystematyzowanie podstawowych wiadomości o systemie EIB i zasygnalizowała możliwości zastosowań tego wygodnego i mającego wiele zalet rozwiązania. W części drugiej zostaną omówione stosowane w tym systemie urządzenia, a w kolejnej – zagadnienia związane z wzajemną komunikacją pomiędzy nimi. Część ostatnia będzie poświęcona zastosowaniom EIB w praktyce

CZĘŚĆ 2. Urządzenia w systemie EIB

Urządzenia sterujące

Przez urządzenie sterujące w systemie EIB rozumie się każde urządzenie, które wysyła sygnał (telegram) do magistrali. Sygnał ten może być wysłany przez urządzenie automatycznie, programowo lub „ręcznie", na skutek interwencji człowieka (np. przez przyciśnięcie przycisku).

W systemie EIB można wyróżnić następujące urządzenia sterujące:

a) przyciski jednokrotne lub wielokrotne, które mogą wykonywać różne funkcje w zależności od zastosowanej wersji programu aplikacyjnego. Przyciski wysyłają informację (telegram) na magistralę po naciśnięciu krótko lub po dłuższym przytrzymaniu. Prawa strona przycisków może działać niezależnie od lewej (podobnie góra i dół przycisku), co można zaprogramować. Bardzo często przyciski wyposaża się w dodatkowe funkcje sterujące. Używając przycisków, można sterować oświetleniem lub żaluzjami,

Rys. 1. Odbiornik podczerwieni montowany w przycisku – przycisk potrójny

b) pasywne czujki ruchu wyposażone w czujniki podczerwieni (PCP). Wysyłają sygnał do magistrali po naruszeniu strefy chronionej, podobnie jak w systemach alarmowych. Czujki ruchu lub obecności wykorzystuje się do sterowania oświetleniem, ogrzewaniem lub w zarządzaniu bezpieczeństwem,

c) odbiorniki sygnałów z pilota podczerwieni IR,

d) regulatory temperatury z termostatami. Regulator wraz z urządzeniami wykonawczymi utrzymuje zadaną temperaturę w pomieszczeniu, może wykorzystywać różne algorytmy sterowania (np. załącz/wyłącz). Regulatory temperatury bardzo często montowane są w przyciskach z możliwością wyświetlania regulowanych parametrów,

e) zegary z możliwością ustawień dziennych, tygodniowych, miesięcznych lub rocznych. Stosowane są w sterowaniu nadrzędnym oświetleniem, ogrzewaniem lub w kontroli dostępu,

f) moduły wejść analogowych – urządzenia przetwarzające sygnał analogowy na informację cyfrową do magistrali EIB. Wykorzystywane są do przetwarzania sygnałów z czujników analogowych, np. temperatury lub natężenia oświetlenia, kanały w tych wejściach mogą być konfigurowane programowo jako znormalizowane napięciowe 0–10 V lub prądowe 0–20 mA,

g) moduły wejść cyfrowych (binarnych) – urządzenia przeznaczone do odczytywania stanu styków przekaźników i przetwarzania ich na sygnał magistrali EIB. Wejścia binarne mogą obsługiwać styki bezpotencjałowe (zwarcie lub przerwa) albo napięciowe – 230 V AC lub 24 V DC,

h) stacja pogodowa – urządzenie złożone, przetwarza dane otrzymywane z uniwersalnego czujnika temperatury, deszczu i siły wiatru na sygnały (telegramy) magistrali EIB,

i) terminal strefy – urządzenie, do którego podłącza się pasywne detektory, jak np. kontaktrony, czujki zbicia szyby, czujki zalania lub dymu.

ELEMENTY PODSTAWOWE

Połączenie z szyną magistralną DC (BA)	Złącze danych RS232	Złącze typu DCF-77
Dławik (DR)	Złącze zewnętrzne (GAT)	Kostki sterujące, logiczne, sprzęgające, kontrolujące
Zasilanie (SV)	Złącze zewnętrzne np. ISDN	Element łączący
Zasilanie zepolone z dławikiem (NG)	Złącze ze sterownikiem programowalnym SPS (PLC)	Filtr zaporowy
Połączenie z linią magistralną (LK), główną lub obszarową (BK)	Złącze z szyną pola	Łącznik (sprzężenie) fazy

URZĄDZENIA STERUJĄCE (SENSORY)

Symbol ogólny; pole oznaczenia konkretnego zastosowania (a), pole fizycznych wielkości wejściowych (b)	Czujnik natężenia oświetlenia	Odbiornik promieni podczerwonych
Czujnik dwustanowy, pole fizycznych wielkości wejściowych (b) np. prądu stałego	Sygnalizator przekroczenia określonej wartości natężenia oświetlenia	Pasywna czujka ruchu, reagująca na podczerwień i czujka ultradźwiękowa
Łącznik (czujnik) przyciskowy	Czujnik temperatury	Sygnalizator
Czujnik przyciskowy ściemniacza oświetlenia	Przełącznik temperaturowy	Zegar, łącznik reagujący na wartość czasu
Odbiorniki promieni podczerwonych z n-pozycyjnym łącznikiem przyciskowym	Czujnik (łącznik) sterujący przyciskowy	Łącznik zegarowy sterujący ze strefami czasowymi
Dekoder promieniowania podczerwonego	Łącznik przyciskowy sterowania żaluzji	Element umożliwiający uruchomienie instalacji specjalnym kluczem
	Nadajnik promieni podczerwonych	Łącznik instalacyjny

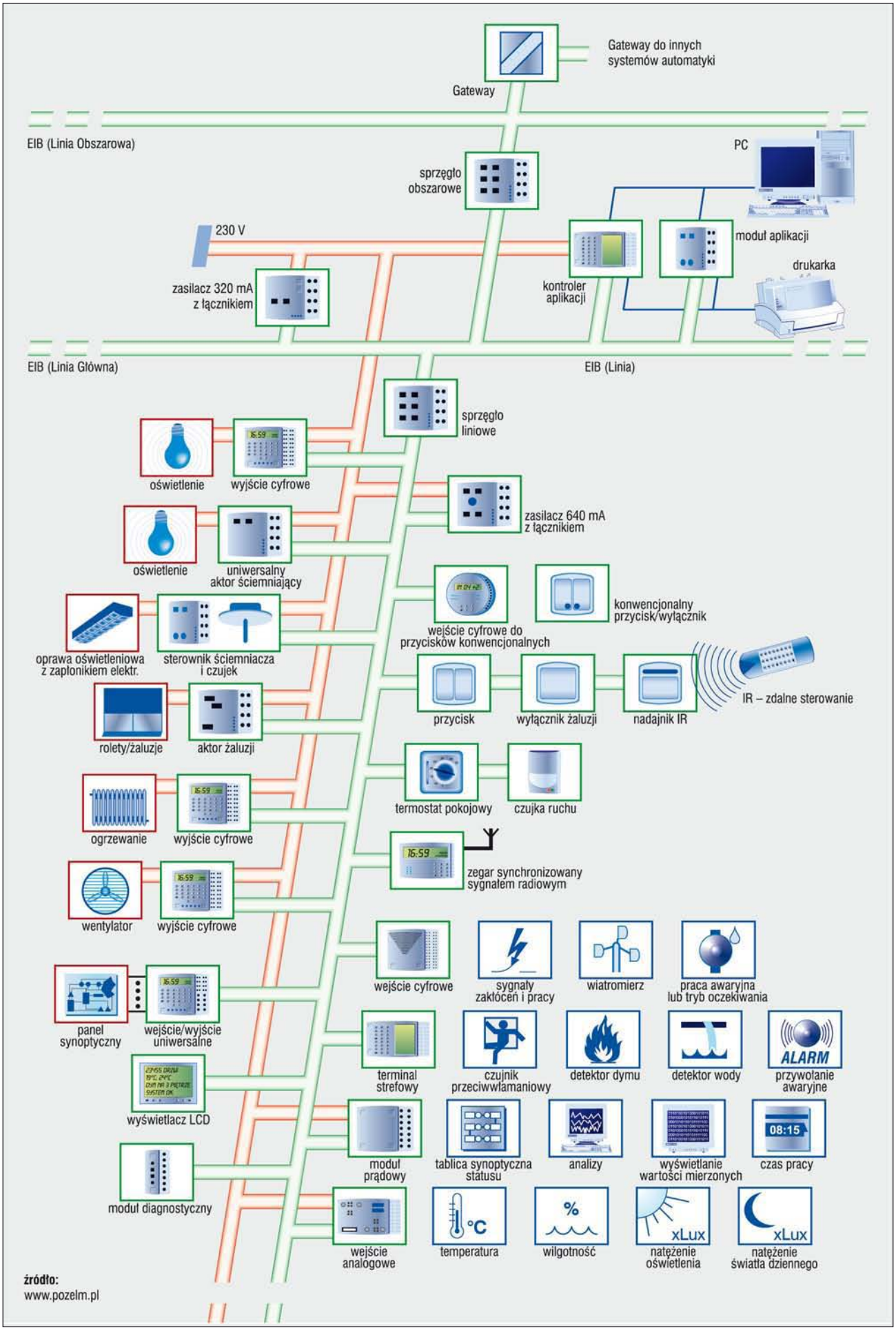
URZĄDZENIA WYKONAWCZE (AKTORY)

Aktor (symbol ogólny)	Łącznik sterowania żaluzjami	Łącznik "taktujący", np. do sterowania zaworów elektrycznych, elektrycznych możliwością nastawienia czasów w poz. ZAŁ i poz. WYŁ
Aktor z napięciem pomocniczym	Aktor (łącznik) ściemniacza oświetlenia	
Aktor działający ze zwłoką czasową	Tablica wyświetlacza, wyświetlacz (display) n-miejscowy	Zawór nastawialny
Aktor (łącznik) dwustanowy załączający	Aktor (wyjście) analogowe, sterownik	Wskaźnik dwustanowy

ELEMENTY ZŁOŻONE

Zestaw czujników temperatury i czasu	Łącznik ze ściemniaczem i wyjściem dwustanowym	Aktor (łącznik) z n-pozycyjnym odbiornikiem podczerwieni
Łącznik dwustanowy z wyjściem dwustanowym	Moduł sprzęgający łącznik czasowy z przełącznikiem reagującym na wartość natężenia oświetlenia	Aktor (łącznik) z n-pozycyjnym łącznikiem przyciskowym

Rys. 2. Symbole elementów magistralnych stosowane na planach instalacji elektrycznych wykonanych w systemie EIB



Rys. 3. Podstawowa struktura systemu EIB

Rys. 4. Ekran dotykowy z nawigacją po systemie EIB

Urządzenia wykonawcze

Urządzenia wykonawcze odbierają sygnały (telegramy) z magistrali EIB i wykonują określone czynności. Mogą działać jak stycznik z możliwymi do wyboru stykami (fazami) do załączenia. Mogą też wytwarzać znormalizowane sygnały analogowe do sterowania dalszymi urządzeniami albo wizualizować informację z magistrali EIB. Aby je określić często używa się w naszym kraju pochodzącego z Niemiec i niezbyt udanego określenia „aktory".

Do urządzeń wykonawczych w systemie EIB zalicza się:

- wielokanałowe moduły wyjść binarnych ze stykami bezpotencjałowymi lub ze stykami obciążanymi prądowo, działające jak inteligentne przekaźniki z programowym wyborem kanału. Możliwe jest wprowadzanie opóźnienia załączenia lub wyłączenia kanału, a także logicznych zależności między kanałami. Urządzenia mogą wysyłać do magistrali tzw. status, czyli informację o stanie styków (a więc o załączeniu lub niezałączeniu urządzenia),
- moduły wyjść analogowych dostarczające znormalizowanych sygnałów analogowych prądowych lub napięciowych, parametry wyjść ustawiane są programowo,
- ściemniacze i sterowniki ściemniania oświetlenia, do regulacji natężenia oświetlenia lamp żarowych lub jarzeniowych. W celu umożliwienia sterowania dużymi grupami lamp stosowane są dodatkowe moduły rozszerzające nawet do mocy około 30 kW w jednej linii,
- sterowniki żaluzji pionowych lub poziomych. Możliwe są dwa tryby pracy w zależności od otrzymanych z magistrali telegramów. Pierwszy rodzaj telegramu powoduje całkowite podniesienie lub opuszczenie rolet, a drugi umożliwia zatrzymanie rolet w trakcie ruchu lub manewrowanie poziomymi lamelami w żaluzjach poziomych. Sterowanie żaluzjami zależy od krótkiego lub długiego w czasie naciśnięcia przycisku sterującego,
- wyświetlacze informacji (rys. 4.), które wyświetlają komunikaty o stanie urządzeń w systemie EIB; niektóre mają możliwość oprócz wizualizacji także modyfikacji parametrów na ekranie komputera.

Na rys. 3. pokazano pełną strukturę systemu rozproszonego EIB. W systemie tym znajduje się duża grupa urządzeń sterujących, które wysyłają komunikaty do magistrali sytemu. Jak widać, czujniki natężenia oświetlenia, temperatury i wilgotności wytwarzają sygnały ciągłe w czasie (analogowe) i dlatego wymagają współpracy z wejściami analogowymi do przetworzenia mierzonej wielkości fizycznej na telegram w magistrali EIB.

Rys. 5. Wizualizacja zdarzeń w systemie EIB przy pomocy oprogramowania do wizualizacji na ekranie komputera

Istnieje też duża grupa czujek zapewniających bezpieczeństwo w zarządzanych budynkach. Należą do niej czujki stłuczenia szyby, czujki wibracyjne, detektory dymu lub gazu oraz przycisk alarmowy przywołania. Dla tej grupy czujek stworzono specjalne urządzenie, tzw. terminal strefowy, który z nią współpracuje.

Czujka ruchu do montażu podtynkowego wewnątrz domu

Bardzo istotną nowością jest możliwość wykorzystania krążących w systemie informacji do wizualizacji procesów w systemie EIB na tablicach synoptycznych lub na ekranach komputerów (rys. 5.).

Ustalenie rodzaju pracy urządzenia sterującego i jego parametrów następuje przy wykorzystaniu przyjaznego oprogramowania ETS (EIB Tool Software).

Urządzenia wykonawcze podłączone są do magistrali EIB, z której otrzymują rozkazy. Dołączona jest do nich też sieć elektroenergetyczna. Zasilanie urządzeń końcowych, np. ogrzewania elektrycznego, wentylatora czy żarówki, następuje poprzez urządzenie wykonawcze EIB.

System EIB dzięki dużej różnorodności urządzeń sterujących i wykonawczych oraz możliwościom monitorowania stał się bardzo atrakcyjnym systemem do zarządzania bezpieczeństwem i komfortem w budynkach.

Znając już najczęściej używane urządzenia sterujące i wykonawcze w systemie EIB, można podać ich symbole, stosowane na schematach elektrycznych projektowanych instalacji. Symbole te zestawiono na rys. 2.

DR HAB. INŻ JERZY MIKULIK – PROF. AGH

Literatura:

1. Kastner D.: *EIB Installation Bus System,* Huethig GmbH, KG, Heidelberg, 2000.
2. *Handbuch Gebäudesystemtechnik. T. 1. Grundlagen, T. 2. Anwendungen*, Frankfurt nad Menem, ZVEI-ZVEH, 1997.
3. Florczykiewicz T., Góralczyk M.: *Automatyczne sterowanie oświetleniem przy wykorzystaniu systemu magistralnego EIBus,* praca dyplomowa mgr, Politechnika Krakowska, 2004.
4. Petykiewicz P.: *Technika systemowa budynku instabus EIB. Podstawy projektowania*, WZ Graf, Warszawa, 1999.
5. Petykiewicz P.: *Nowoczesna instalacja elektryczna w inteligentnym budynku,* COSiW SEP, Warszawa, 2001.
6. Mikulik J., Jakubas W.: *Badania sygnałów w magistrali systemu EIB,* 2nd International Congress on Intelligent Building Systems, Politechnika Krakowska, Kraków, 2002.
7. Materiały firmowe ABB.

Redakcja dziękuje firmie ABB za udostępnienie fotografii.

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

Przegląd czujek wielodetektorowych

POLON-ALFA

sponsorowany

Czujki wielodetektorowe na szerszą skalę zaczęły pojawiać się w ofercie producentów, gdy nastąpił znaczący postęp technologiczny w produkcji podzespołów elektronicznych. Szczególnie pojawienie się stosunkowo tanich i energooszczędnych mikrokontrolerów umożliwiło rozwój tego rodzaju czujek

Dlaczego konstruuje się czujki wielodetektorowe? Wydaje się, że są dwa główne powody:

1. Pojedyncza czujka może wykrywać więcej różnych typów pożarów.
2. Pożary mogą być wykrywane wcześniej, bez zwiększenia podatności czujek na zjawiska zakłócające (powodujące fałszywe alarmy).

Oczywiście czujka wielodetektorowa wykryje tylko takie pożary, gdy emitowane są czynniki, na które reaguje przynamniej jeden z jej detektorów. Dla przykładu, czujka optyczna dymu i ciepła w przypadku pożaru, podczas którego występuje dym, bez wyraźnego wzrostu temperatury, będzie zachowywać się jak czujka dymu. Niemniej jednak pojawienie się obu czynników jednocześnie spowoduje, że zadziałają oba zastosowane w czujce detektory co w konsekwencji przyspieszy alarm pożarowy.

Pierwszymi produkowanymi na szerszą skalę czujkami wielodetektorowymi były czujki dymu i ciepła. Czujki te posiadają optyczny detektor dymu i czujnik ciepła w postaci termistora.

Klasyczna czujka optyczna dymu dobrze wykrywa pożary emitujące jasny, widzialny dym. Są to pożary typu TF2, TF3 i TF4. Pożarów typu TF1 jak i TF6 klasyczna czujka optyczna nie wykrywa. Może mieć problemy z pożarem TF5. W tab. 1. zaprezentowano zestawienie pożarów testowych (z podziałem na rodzaj spalanego materiału) oraz dominujące czynniki towarzyszące (zgodnie z ISO/TS 7240-9).

Można powiedzieć, że klasyczna optyczna czujka dymu dobrze wykrywa pożary tlewne, ma natomiast problemy z pożarami płomieniowymi. Producenci różnymi zabiegami (np. poprzez zwiększenie czułości) starali się poprawiać charakterystykę tych czujek. Jednak mogło to mieć wpływ na zwiększenie ich podatności na wywoływanie fałszywych alarmów. Przydatność optycznej czujki dymu do wykrywania pożarów testowych przedstawiono w tab. 2 (użyte w niej, a także w następnych tabelach symbole oznaczają, że dana czujka jest: A – bardzo przydatna, B – przydatna, C – jeszcze przydatna, N – nieprzydatna).

Podczas pożarów płomieniowych wydziela się dostateczna ilość ciepła, która powoduje mierzalny wzrost temperatury tanich detektorów (termistorów). Dlatego dodając do czujki dymu detektor ciepła, można poprawić charakterystykę czujki dymu dla pożarów płomieniowych.

Test	TF1	TF2	TF3	TF4	TF5
DOR-40	N	B	B	B	C

Tab. 2. Przydatność optycznej czujki dymu do wykrywania pożarów testowych

Norma PN-EN 54-7 obejmuje czujki optyczne dymu o czułościach m≥0,05 dB/m (im parametr m większy, tym mniejsza czułość). Nie obejmuje czujek czulszych. W praktyce nie produkuje się czujek o czułości nawet zbliżonej do 0,05 dB/m. Tak czułe czujki są niezwykle podatne na zakłócenia: dym papierosowy, parę wodną, kurz itp.

W normalnych warunkach czułość czujek optycznych dymu produkowanych przez Polon-Alfa zawiera się w przedziale od 0,2 do 0,3 dB/m. W przypadku wielodetektorowej czujki dymu i ciepła można dynamicznie zwiększyć czułość detektora dymu, jeżeli w tym samym czasie drugi z detektorów, detektor ciepła, wykrył narost temperatury. Zwiększenie czułości członu dymowego w takim przypadku nie zwiększa podatności czujki do wywoływania fałszywych alarmów. Zakładamy bowiem, że prawdopodobieństwo wystąpienia zjawisk zakłócających oba detektory w tym samym czasie jest znikome. Oczywiste jest, że w miejscach, gdzie takie zjawisko może nastąpić, nie należy stosować tego typu czujek. Przykładem może być kotłownia, w której otwarcie drzwiczek paleniska może spowodować zarówno nagły przyrost temperatury, jak i zadymienia.

Podobne rozumowanie można przeprowadzić także dla detektora ciepła. Czułość detektora ciepła zostaje podniesiona znacznie powyżej ograniczeń stawianych przez normę PN-EN 54-5, jeżeli w tym samym czasie detektor dymu wykryje wzrost jego koncentracji.

Nie wdając się w rozważania matematyczne i skomplikowane algorytmy działania, które są implementowane w mikrokontrolerach czujek, z punktu widzenia użytkownika optyczna czujka dymu i ciepła przy wykryciu narostu temperatury

Test	TF1	TF2	TF3	TF4	TF5	TF6	TF8
Rodzaj pożaru testowego	płomieniowe spalanie drewna	rozkład termiczny (piroliza) drewna	pożar tlewny bawełny	płomieniowe spalanie tworzywa (poliuretanu)	spalanie cieczy (n-heptan) wydzielającej dym	spalanie cieczy (alkohol etylowy) niewydzielającej dymu	spalanie cieczy (dekalina) wydzielającej dym
Dominujące czynniki pożarowe	otwarty płomień, dym słabo widoczny, silny wzrost temperatury	jasny dym rozpraszający, o małej prędkości wznoszenia	jasny dym rozpraszający, o bardzo małej prędkości wznoszenia	bardzo ciemny dym, wzrost temperatury	bardzo ciemny dym, wzrost temperatury	silny wzrost temperatury	ciemny dym, niewielki wzrost temperatury

Tab. 1. Porównanie pożarów testowych

zachowuje się tak jak czujka dymu ze znacznie podniesioną czułością.

Należy podkreślić, że dla pożarów, podczas których nie są emitowane jednocześnie dym i ciepło, wielodetektorowe czujki dymu i ciepła zachowują się tak jak pojedyncze czujki. W czasie pożarów tlewnych (TF2, TF3) brak jest mierzalnej przez termistor emisji ciepła, czyli dla tych pożarów czujka dymu i ciepła będzie zachowywać się jak optyczna czujka dymu. Podczas pożaru TF6 nie wydziela się dym, dlatego w przypadku takiego pożaru wielodetektorowa czujka dymu i ciepła będzie zwykłą czujką ciepła.

Pamiętać należy także o ograniczeniach w stosowaniu czujek wielodetektorowych. Jeżeli detektory zastosowane w czujce mają różne dozwolone wysokości instalowania, to dopuszczalna wysokość zainstalowania czujki wielodetektorowej jest wartością najmniejszą. Przykładowo, powyżej 8 m czujka dymu i ciepła staje się zwykłą czujką dymu. Podobne zasady obowiązują przy wyznaczaniu wielkości obszaru nadzorowanego.

Firma Polon-Alfa produkuje następujące wielodetektorowe czujki dymu i ciepła:

1. DOT-4046 – czujka adresowalna do central systemu POLON 4000
2. DOT-40 – czujka konwencjonalna do central systemu IGNIS 1000

W tab. 3. przedstawiono porównanie przydatności optycznej czujki dymu DOR-40 oraz wielodetektorowej czujki dymu i ciepła DOT-4046 do wykrywania pożarów testowych.

Podczas testowych pożarów płomieniowych, oprócz wydzielania się dymu (oczywiście z wyjątkiem pożaru TF6) i ciepła, emitowane jest także promieniowanie podczerwone. W związku z tym zamiast detektora ciepła można użyć detektora podczerwieni jako drugiego, obok detektora dymu, detektora w czujce, który będzie spełniał podobną rolę jak termistor. Firma Polon-Alfa jako pierwsza w świecie wprowadziła do sprzedaży w 2004 roku wielodetektorową czujkę dymu i płomienia DPR-4046. Promieniowanie podczerwone rozchodzi się szybciej od narastania temperatury, zatem czujka DPR-4046 dla pożarów płomieniowych wykazuje większą przydatność niż czujka typu DOT. Porównanie przydatności w pożarach testowych czujek DOT-4046 i DPR-4046 przedstawia tab. 4.

Z tabeli wynika przewaga czujki DPR-4046 dla pożarów TF1, TF4, TF8. Czujka optyczna dymu i płomienia ma dla tych pożarów przydatność taką jak czujka jonizacyjna dymu.

Czujka jest nieprzydatna dla pożaru TF6. Założeniem konstrukcyjnym czujki DPR-4046 było, by jej cena nie odbiegała znacząco od ceny czujki DOT-4046. Aby to osiągnąć, należało zastosować w niej detektor promieniowania podczerwonego, którego cena niewiele różniłaby się od ceny termistora. Taka stosunkowo tania konstrukcja detektora ma tę wadę, że w pewnych sytuacjach można zakłócić jego pracę. Zastosowanie bardziej złożonego detektora płomienia podniosłoby cenę czujki kilkunastokrotnie. Dlatego czujka powinna pracować w trybie wielodetektorowym a detektor płomienia nie może samodzielnie wprowadzać jej w stan alarmu pożarowego. Pracując w tym trybie, czujka ma bardzo wysoką czułość na pożary dymowo-płomieniowe. Na uwagę zasługuje fakt, że detektor płomienia spełnia całkowicie normę PN-EN 54-10 (czujki płomienia), co jest potwierdzone wielokrotnymi badaniami w naszym laboratorium jak i Laboratorium BA w CNBOP.

Nowością w ofercie firmy POLON-ALFA jest czujka TOP-40. Jest to dwustanowa, wielodetektorowa czujka ciepła i płomienia. Szczególnie polecana jest do stosowania w miejscach gdzie ze względu na panujące warunki nie można stosować czujek dymu, tzn. w pomieszczeniach, w których stale lub okresowo panuje zadymienie, zapylenie itp. Do tej pory w miejscach takich stosowano najczęściej zwykłe czujki ciepła. Dodanie do czujki ciepła detektora podczerwieni i opracowanie specjalnych algorytmów pracy znacznie zwiększyło jej czułość na pożary płomieniowe, czujka zachowała dużą odporność na zakłócenia. Dla pożarów płomieniowych można ją nawet klasyfikować tak jak czujki dymu. Wyniki pomiarów w komorze pożarów testowych przedstawia tab. 5.

Test	TF1	TF2	TF3	TF4	TF5	TF6	TF8
DOR-40	N	B	B	B	C	nie badano	nie badano
DOT-4046	B	B	B	B	B	B	B

Tab. 3. Porównanie przydatności optycznej czujki dymu DOR-40 oraz wielodetektorowej czujki dymu i ciepła DOT-4046 do wykrywania pożarów testowych

Test	TF1	TF2	TF3	TF4	TF5	TF6	TF8
DOT-4046	B	B	B	B	B	B	B
DPR-4046	A	B	B	A	B	N	A

Tab. 4. Porównanie czujek DOT-4046 i DPR-4046

Test	TF1	TF4	TF5	TF6	TF8
TOP-40	A	C	B	A	N

Tab. 5. Przydatność czujki TOP-40 do wykrywania pożarów testowych

Zastosowany w czujce TOP-40 detektor ciepła jest klasy A1R wg PN-EN 54-5, a detektor płomienia jest klasy 2 (17 m) wg PN-EN 54-10. Zastosowane sposoby detekcji pożaru są adekwatne do warunków, w których przewidziana jest praca czujki. Zarówno ciepło, jak i promieniowanie podczerwone emitowane przez pożary płomieniowe nie są maskowane przez zadymienie lub zapylenie. Ponadto stopień ochrony obudowy czujki IP 44 został również dobrany pod kątem pracy w trudnym środowisku.

Podobnie jak w czujce DPR-4046 człon płomieniowy podczas pracy wielodetektorowej nie może samodzielnie wprowadzić czujki TOP-40 w stan alarmu pożarowego, jednak spełnia całkowicie normę PN-EN 54-10 (czujki płomienia).

Ciekawym rozwiązaniem jest sposób okresowego sprawdzenia poprawności działania czujki. Oprócz tradycyjnego, polegającego na przestawieniu czujki w tryb niezależnej pracy dwóch sensorów, przez wyjęcie specjalnej zworki serwisowej (wymaga wyjęcia czujki z gniazda i ponownego włożenia) i spowodowania zadziałania każdego z detektorów osobno za pomocą imitatora ciepła i imitatora płomienia, istnieje sposób testowania bez wyjmowania czujki z gniazda. Jeżeli czujka jest zainstalowana w trudnodostępnym miejscu, należy wyłączyć zasilanie linii dozorowej, do której podłączona jest czujka TOP-40, odczekać pięć minut i ponownie włączyć zasilanie. Przez pierwsze dwie minuty od włączenia zasilania czujka jest w trybie niezależnego działania dwóch sensorów i można sprawdzić każdy sensor indywidualnie.

Czujka TOP-40 jako dwustanowa przewidziana jest do bezpośredniej współpracy z konwencjonalnymi centralami systemu IGNIS 1000. Do central systemu POLON 4000 można ją podłączyć przez adapter linii bocznej ADC-4001M.

Lech Światły
Polon-Alfa

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

Dwukierunkowa klawiatura

Sygnalizator zewnętrzny

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

OFICJALNI DYSTRYBUTORZY:
ALPOL: Warszawa Mokotów, Warszawa Praga, Katowice, Kraków, Łódź, Wrocław, Poznań, Szczecin, Bielsko-Biała, Gliwice, Lublin, Sopot;
ASD Systemy Zabezpieczeń: Łódź; **ELEKTRON:** Kraków; **INTERFACH2:** Radom; **PATRONIC:** Szczecin, Gorzów Wielkopolski, Zielona Góra, Jelenia Góra;
PROXIMA ALARM GROUP: Toruń; **SOLAR POLSKA:** Łódź, Kraków, Lublin, Poznań, Szczecin, Wrocław; **SPS TRADING:** Warszawa, Łódź, Wrocław, Poznań

ZAGROŻENIE PODSŁUCHEM

bezprzewodowych radiowych klawiatur komputerów

Nawet fachowcom od bezpieczeństwa komputerowego umyka pewna bardzo istotna zmiana, która zaszła w tej dziedzinie na początku obecnego wieku. Zmieniło się mianowicie w sieciach firmowych położenie informacji, które potencjalni napastnicy uznają za atrakcyjne. Jeszcze kilka lat temu uważano, że najcenniejsze dane w sieciach firmowych zlokalizowane są na serwerach i tak było w istocie. Do dziś pokutuje przekonanie, że szczególnym sukcesem napastnika jest włamanie na serwer i serwerom poświęca się najwięcej miejsca w instrukcjach i poradnikach konfiguracji, stacje robocze traktując po macoszemu. Tymczasem w większości firm na serwerach znajdują się informacje cenne dla firmy, których utrata zapewne byłaby niezwykle dotkliwa, ale dla napastnika dane te nie są specjalnie atrakcyjne. Za to dane wprowadzane przez operatorów niektórych stacji roboczych mogą okazać się dla intruza bezcenne.

W znacznym uproszczeniu można powiedzieć, że na serwerach firm z informacji szybko zamienialnych na gotówkę pozostały już tylko bazy danych klientów firmy. Nawiasem mówiąc, najłatwiej są one osiągalne ze stacji roboczych pracujących w sieci. Dlatego najtańszym sposobem zdobycia takiej bazy danych jest skorumpowanie możliwie mało znaczącego pracownika, z którego komputera jest dostęp do bazy, a potem już tylko oczekiwanie, aż zapuszczony na tym komputerze skrypt powoli, drogą kolejnych zapytań, skompletuje potrzebne dane. Oczywiście dla niektórych napastników – na przykład policjantów (także skarbowych) prowadzących czynności dochodzeniowe w firmie w sprawie gospodarczej – zasoby z serwerów mogą jednak być atrakcyjne.

Obecnie stacje robocze stały się celem niezwykle atrakcyjnym, choć specjaliści od bezpieczeństwa nie zawsze to zauważają. W szczególności dotyczy to tzw. stacji decyzyjnych: komputerów VIP-ów lub ich asystentek. Łatwo sobie wyobrazić korzyści z dostępu do zasobów stacji roboczej w sekretariacie prezesa wielkiej spółki akcyjnej – można poznać treść dokumentów przygotowywanych na zebrania zarządu, zanim zapoznają się z nimi decydenci. Zyskamy około dwóch tygodni na zebranie środków i inwestycje giełdowe, zanim decyzje zostaną oficjalnie opublikowane. Korzyści zależą tylko od środków zainwestowanych w grę giełdową. Zapewne konkurenci spółki zapłacą również za możliwość monitorowania decyzji jej zarządu...

Stacje robocze mogą być skutecznie atakowane w różny sposób – zwykle dzięki wykorzystaniu błędów oprogramowania lub przez oszukiwanie operatora. Tzw. wormy (robaki sieciowe) i inne oprogramowanie złośliwe codziennie dowodzą swojej skuteczności. Wormy mają jednak tę przewagę nad gotującym się do ataku na upatrzoną firmę hakerem, że nie muszą wybierać ofiar – każda jest dobra. Jednak haker, który chciałby się dobrać do informacji jakiejś firmy, czy wręcz do konkretnego komputera, jest w znacznie trudniejszej sytuacji. Z drugiej strony, rozwój techniki otwiera nowe możliwości przed napastnikami – jedną z nich jest, nieosiągalna dla wormów, możliwość podsłuchu emitowanych przez sprzęt komputerowy fal radiowych. Dotyczy to w szczególności klawiatur radiowych.

W niniejszym artykule przedstawione zostaną konkluzje z badań prowadzonych na Wydziale Cybernetyki Wojskowej Akademii Technicznej, nad urządzeniami bezprzewodowo (drogą radiową) komunikującymi się z jednostką centralną komputera. Wnioski dotyczą przede wszystkim możliwości podsłuchu klawiatur radiowych.

Dlaczego właśnie klawiatura?

W dawnych pracach nad wrażliwością systemów komputerowych jeden z autorów rozważał, jak można najskuteczniej dobrać się do informacji stacji roboczej, której operator może tworzyć lub edytować dokumenty zawierające pożądaną informację. Rozważając model warstwowy systemu komputerowego (obejmujący jego elementy sprzętowe i oprogramowanie), można wskazać następujące drogi przesyłania lub miejsca przechowywania informacji w komputerze:

- dyski (pamięć masowa) komputera, montowane wewnątrz obudowy bloku głównego,
- droga do monitora, emisja ujawniająca z monitora,
- droga do drukarki, emisja ujawniająca z drukarki (związana z drukowaniem),
- sieć przewodowa,
- sieć bezprzewodowa,
- droga z klawiatury przyłączonej kablem, przez wejście PS2 lub USB,
- droga z klawiatury radiowej.

Można ocenić atrakcyjność ataków na każde z tych miejsc, jak to przedstawia tab. 1, rozpatrując następujące cechy tych ataków:

1. Informacyjność – to cecha ilustrująca nasycenie przesyłanego sygnału (lub zapisu na nośniku) użyteczną dla napastnika informacją. Interesująca napastnika informacja przechwycona z połączenia z monitorem będzie znacznej objętości, ta sama przechwycona z klawiatury będzie zajmować znacznie mniej miejsca. Można przypuszczać, że przechwycenie sygnału wysoce informacyjnego będzie bardziej atrakcyjne dla napastnika niż „niskoinformacyjnego". Okazuje się, że informacja przesyłana do/z klawiatury jest najbardziej „nasycona informacją". To naturalne, że aktualne dokumenty są wprowadzane z klawiatury, a właśnie na takich dokumentach napastnikowi zależy najbardziej. Najgorszą wartość ten parametr przyjmuje dla monitora.

2. Szanse na napotkanie atrakcyjnej dla napastnika informacji w przesyłanym sygnale lub na nośniku. Ogólnie można się spodziewać, że aktualna informacja z pewnością znajdzie się na dysku, zapewne będzie wprowadzana z klawiatury, być

może zostanie wydrukowana, zaś przesłanie jej przez sieć nastąpi tylko w wyjątkowych przypadkach.

3. Bezinwazyjność – to cecha, która charakteryzuje zakres koniecznych zmian w komputerze ofiary (w jego strukturze sprzętowej lub oprogramowaniu) niezbędnych dla powodzenia ataku. Dla napastnika najbardziej atrakcyjne będą oczywiście ataki całkowicie bezinwazyjne – nie wymagające wprowadzenia zmian, co jest osiągalne w przypadku podsłuchu ulotu elektromagnetycznego, podsłuchu sieciowego w sieciach bezprzewodowych lub przewodowych, w których koncentratorem jest hub (*ARP spoofing* lub inną technikę *man-in-the-middle* należy uznać za zmianę w połączeniu). Za inwazyjne uznane powinny zostać wszystkie techniki wymagające instalacji specjalnego oprogramowania – zmierzającego do przejęcia informacji, a następnie wyprowadzenia jej do napastnika; absolutnie bezinwazyjne techniki zapewniają praktyczną niewykrywalność ataku. Klawiatura radiowa zajmuje tu zaszczytne pierwsze miejsce (*ex aequo* z siecią WiFi).

4. Brak szyfrowania – oznacza spodziewany brak ochrony kryptograficznej przesyłanej (lub pamiętanej) informacji; informacja przesyłana z klawiatury nie jest szyfrowana, a sposób kodowania sygnału jest stosunkowo prosty;

5. Ukrycie – charakteryzuje stopień trudności wykrycia wprowadzonych przez napastnika zmian w obiekcie, niezbędnych dla powodzenia ataku; wartość tej cechy należy uznać za maksymalną dla ataków bezinwazyjnych (ukrycie absolutne chociażby z tej racji, że nieistniejących zmian wykryć się nie da – uzasadnienie formalnie zapewne niepoprawne, ale w praktyce oczywiście prawdziwe).

Im „bardziej dodatnie" określenia w każdym z wierszy, tym bardziej atrakcyjne dla napastnika odpowiednie połączenie. Tab. 1, jak widać, wskazuje jednoznacznie zwycięzcę – z punktu widzenia napastnika najodpowiedniejsze jest zdobywanie informacji pobieranej przez aplikację z klawiatury, zwłaszcza bezprzewodowej. Główną konkluzją z tego przeglądu jest to, że **informacja przesyłana z klawiatury bezprzewodowej do stacji bazowej (podłączonej kablem do komputera) to marzenie szpiega**: daje możliwość biernego – niewykrywalnego podsłuchu, a informacja wpisywana przez operatora przesyłana jest znak po znaku, zatem właściwie bez możliwości efektywnego szyfrowania blokowego. Co prawda trzeba przyznać, że tab. 1 jest cokolwiek tendencyjna – nie obejmuje cechy precyzji wyników, mierzonej np. podobieństwem pozyskanych dokumentów do ich pierwowzorów. W tym zaś rankingu na pierwszym miejscu znajduje się drukarka i monitor, a na szarym końcu klawiatura bezprzewodowa. Na szczęście dla napastnika ta różnica nie jest znowu aż tak wielka, aby uniemożliwić pozyskanie interesującej informacji – najwyżej jej postać nie będzie doskonała.

Skoro mowa o przemilczanych wadach ataku na klawiaturę, można przypomnieć, że istnieją takie postaci informacji, które nie są wprowadzane ani edytowane za pomocą klawiatury – to rysunki, obrazy, zapisy dźwięku czy filmy. Pozostaną one niedostępne dla napastnika. Podobnie przeszkodę w skompletowaniu obrazu dokumentu stanowić mogą także sytuacje, gdy dokument nie jest tworzony od początku, a jedynie poprawiany przez operatora.

W ogólności do prób zdobycia informacji pobieranych przez aplikacje z klawiatury można użyć różnych narzędzi:
- dowolnego narzędzia do podsłuchu „z powietrza" sygnału radiowego,
- skrycie zainstalowanego programu przechwytującego wszystkie wciskane klawisze (to tzw. *keylogger* lub *key thief*) lub
- modyfikacji sprzętowych (klawiatury lub kabla) wprowadzonych w komputerze ofiary.

Ostatni z wymienionych sposobów to wprowadzenie modyfikacji sprzętowych przez zamontowanie w klawiaturach komputerów (lub jednostkach centralnych) niewielkich urządzeń nadawczych. Wymagałoby to wprowadzenia własnej ekipy na teren ofiary, po czym wykorzystania braku nadzoru, działania pod pretekstem dokonania naprawy lub szybkiej podmiany klawiatury. Alternatywą jest wypróbowanie praktykowanego ponoć przez szpiegów gospodarczych sposobu na podsłuch telefoniczny: dostarczania konkurencyjnej firmie superatrakcyjnych telefonów komórkowych z najwyższej półki w ramach promocji, oczywiście telefonów odrobinę zmodyfikowanych... To samo można zrobić z klawiaturą, ale szansa na trafienie jej w pożądane miejsce jest dużo niższa niż w przypadku telefonu komórkowego.

Emisja fal radiowych – zjawisko nie zawsze niepożądane

Problem niepożądanej emisji elektromagnetycznej jest znany od dawna. Poświęcono mu liczne publikacje, a zapewne równie wiele, i to znacznie ciekawszych opracowań, pozostało utajnionych z racji ich związku z ochroną informacji niejawnych. Wystarczy wspomnieć tylko powszechnie znany kryptonim „Tempest". Na wstępie warto podkreślić różnice w traktowaniu emisji elektromagnetycznej:

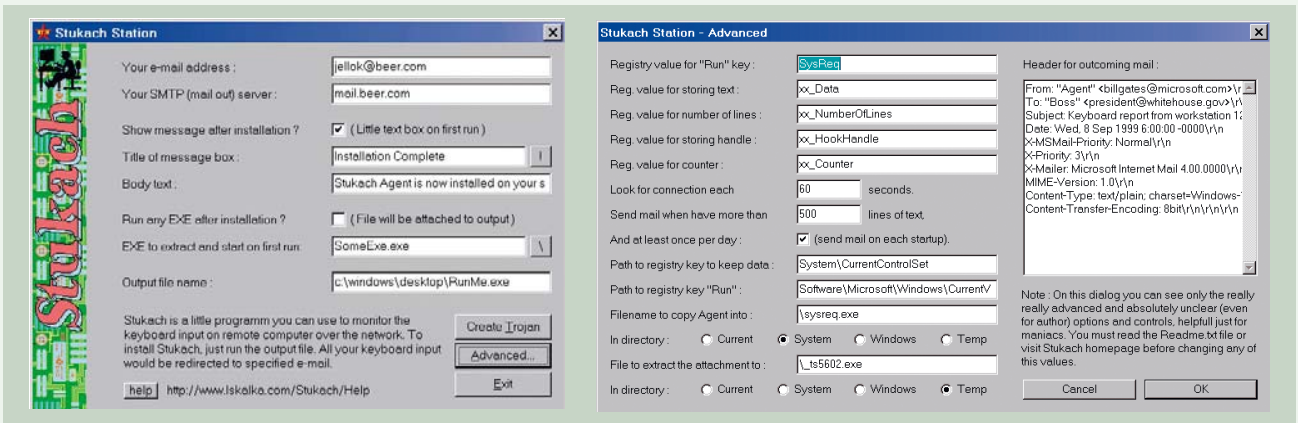
1. W przypadku „klasycznych" komputerów emisja jest zjawiskiem niepożądanym i bezwzględnie zwalczanym – zarówno ujawniająca, jak i zakłócająca.

Urządzenie	Nasycenie informacją	Szanse	Bezinwazyjność	Brak szyfrowania	Ukrycie
Klawiatura radiowa	wysokie	duże	tak	tak	absolutne
Klawiatura	wysokie	duże	nie	tak	średnie
Sieć przewodowa	niskie/brak	małe	różnie	nie	dobre
Sieć bezprzewodowa	niskie/brak	małe	tak	nie	absolutne
Monitor	bardzo niskie	bardzo duże	raczej nie	kodowanie	słabe
Drukarka	niskie	średnie	nie	kodowanie	średnie
Dysk	średnie	bardzo duże	nie	tak	słabe

Tab. 1. Ocena dróg informacji w systemie z punktu widzenia napastnika

2. W przypadku sieci bezprzewodowych emitowany sygnał roboczy powinien być możliwie czysty i o jak największym zasięgu.
3. W przypadku urządzeń zewnętrznych komunikujących się drogą radiową z komputerem pożądane jest uzyskanie czystej, niezakłóconej transmisji w założonym zasięgu pracy urządzenia, najlepiej ograniczonym do niewielkiej strefy obejmującej urządzenie i nadawczo-odbiorczą jednostkę sterującą. Poza tą strefą emisja jest niepożądana.

Keyloggerów w Internecie jest zatrzęsienie (por. [3]), ale dla ilustracji najlepiej nadaje się klasyczny keylogger o nazwie *Stukach*. Rys. 1 przedstawia dwa okna sterujące programu *Stukach Station*. To generator programów instalacyjnych, które instalują tzw. agenta stukacha o parametrach pożądanych przez operatora. Łatwo zauważyć, że operator tego programu może wybrać nazwy dla programu instalacyjnego i dla przyszłego agenta, lokalizację zarówno agenta, jak i pliku gromadzonych danych, miejsca wpisu do rejestru itd. Na pierwszym ekranie wi-



Rys. 1. Stukach Station – okna sterujące

Łatwo zauważyć, że ten ostatni przypadek jest szczególnie niewygodny dla projektantów, co zdaje się otwierać nowe perspektywy przed intruzami. Skoro, jak wspomniano, tyle napisano o niebezpieczeństwie niepożądanej emisji elektromagnetycznej (przypadek pierwszy na liście powyżej), można się spodziewać, że celowe wysyłanie silnego sygnału w eter dopiero pozwoli na podsłuchiwanie! Doświadczenia z sieciami bezprzewodowymi zadają się potwierdzać to rozumowanie.

Klasyczne narzędzia – keyloggery

Interesującymi narzędziami ataku na stacje robocze są keyloggery – programy do przechwytywania informacji z klawiatury. Używane są do różnych celów, zarówno legalnych (np. do monitorowania zdarzeń lub nadzoru nad pracownikami), jak i nie. Ten ostatni przypadek bardziej pasuje do tematu niniejszego tekstu jako alternatywne narzędzie do podsłuchu klawiatury. Dobry keylogger tego rodzaju (czyli szpiegowski) powinien rejestrować wszystkie wciskane klawisze, łącznie ze sterującymi, poddawać plik zebranych danych kompresji, szyfrować go i wysyłać (na przykład pocztą) pod wskazany adres. Niektóre wersje rejestrują również nagłówek okna przy zmianie okien oraz przeniesienia kursora za pomocą myszki. Na komputerze ofiary instalowany jest skrycie program (nazywany także agentem keyloggera), który powinien być trudno wykrywalny.

Jeśli agent nie ma być instalowany ręcznie, zwykle występuje pewien program instancyjny, najczęściej udający zupełnie inny lub z innym programem „zbindowany". Program instalacyjny jest preparowany tak, aby można było łatwo nakłonić operatora atakowanego komputera do uruchomienia go – np. jest przesyłany jako atrakcyjna gra lub niecierpiąca zwłoki ważna poprawka do systemu. Istotą działania programu instalacyjnego jest skryte – niedostrzegalne dla operatora atakowanego komputera – osadzenie agenta keyloggera. Skojarzenie z koniem trojańskim jest tu całkowicie na miejscu.

dać adres pocztowy, pod który mają być wysyłane gromadzone dane, zaś na drugim można ustawić wiersze początkowe wysyłanego maila; przed wierszem „From:" użytkownik o większej wyobraźni może dodać kilka wierszy „Received". Warto zauważyć, że poczta wysyłana jest w protokole SMTP bezpośrednio do wskazanego serwera pocztowego, co pozwala ominąć lokalne mechanizmy nadzoru poczty, oczywiście jeśli pozwalają one na połączenia zewnętrzne na port poczty (25).

Stukach jest doskonałym narzędziem, jego obsługa nie wymaga specjalnych umiejętności. Mógłby być skutecznie wykorzystywany przez tzw. *script kiddies* gdyby nie to, że jest doskonale znany programom antywirusowym. Podkreślić jednak trzeba, że dla specjalisty przerobienie programów rozpoznawanych przez antywirusy na wersje niewykrywalne nie stanowi problemu. Modyfikacja tzw. sygnatur wirusowych – fragmentów kodu, na podstawie których monitory antywirusowe identyfikują niepożądane programy – wymaga kwalifikacji odpowiadającym mniej więcej umiejętnościom studenta drugiego roku informatyki, jeśli program studiów obejmuje asembler.

Problemem jest ukrycie w systemie osadzonego keyloggera. Można się również spodziewać, że po wykryciu jego obecności napastnik będzie zagrożony: prowadzący dochodzenie pójdą tropem wysyłanej przez keylogger informacji – do komputera napastnika. O ile oczywiście ten ostatni nie podjął należytych środków[1] zmierzających do zapewnienia sobie anonimowości.

Keyloggery okazują się znakomitymi narzędziami pomocniczymi także podczas podsłuchu klawiatur radiowych „z powietrza".

1) Najprostszy ich zestaw to: wskazanie anonimowego konta na którymś z dużych, darmowych serwerów (np. Hotmail lub Yahoo) i odczytywanie informacji z tego konta za pośrednictwem jednego lub kilku anonimowych serwerów proxy, najlepiej położonych w krajach, między którymi nie ma tradycji współpracy organów ścigania.

Podsłuch „z powietrza”

Podsłuch sygnałów związanych z przyciskaniem klawiszy klawiatury jest możliwy dzięki rejestrowaniu fal radiowych emitowanych przez klawiaturę bezprzewodową w ramach komunikacji jej modułu klawiatury ze stacją bazową – niewielkim urządzeniem podłączonym do klawiaturowego gniazda PS2 lub do gniazda USB komputera. Oczywiście możliwe jest również rejestrowanie niepożądanej emisji elektromagnetycznej towarzyszącej działaniu elektroniki klawiatury.

W przypadku klawiatury bezprzewodowej sygnał roboczy komunikacji między klawiaturą a bazą przesyłany jest albo zgodnie ze standardem Bluetooth (tzw. profile K5 lub K13, inne niż w telefonach komórkowych), albo według reguł wybranych przez konstruktorów dla tej jednej konstrukcji (typu) urządzenia. Obecnie[2] oferta rynkowa klawiatur Bluetooth w polskich sklepach internetowych to kilka modeli (na ponad 800 oferowanych), wszystkie w cenie powyżej 600 zł, gdy ceny pozostałych klawiatur radiowych (z myszką) to średnio poniżej 100 zł [11].

Klawiatury bezprzewodowe zgodne ze standardem Bluetooth działają na częstotliwości 2,4 GHz, pozostałe zwykle na częstotliwościach poniżej 1 GHz. Dla klawiatur bezprzewodowych poza Bluetooth nie zostały jeszcze ustalone standardy połączeń radiowych. W tych urządzeniach można się spodziewać prostego protokołu punkt–punkt, dalece różniącego się od złożonych protokołów sieciowych. Ze względów ekonomicznych zapewne nie wystąpią również konstrukcje z dokładną separacją i uzgadnianiem kanałów. Dotychczasowe badania dostępnych klawiatur wykazują, że tak jest w istocie.

Pierwszym eksperymentem przeprowadzonym przez autorów niniejszego opracowania było umieszczenie w pobliżu podsłuchiwanego komputera z radiową klawiaturą drugiego komputera wyposażonego w identyczną stację bazową klawiatury (urządzenie nadawczo-odbiorcze dołączane do gniazda klawiatury). Osiągnięto spektakularny sukces – drugi komputer rejestrował całość sterowania za pomocą klawiatury (co ciekawe – bezprzewodowej myszki również) z pierwszego komputera.

Jak z tego wynika, **atak przez podsłuch radiowej klawiatury to w większości przypadków działanie dziecinnie proste**. Wystarczy:

- zapakować do teczki notebook z podłączonym urządzeniem bazowym identycznego typu, w jakie wyposażony jest komputer ofiary,
- włączyć program rejestrujący wciskane klawisze (najlepiej keylogger, ale wystarczy Notatnik lub np. MS Word) na notebooku i zbliżyć się, aby wejść w zasięg emisji klawiatury.

Zostaną zarejestrowane wszystkie wciśnięcia klawiszy. Także początkowe hasła systemowe (które są zwykle nieosiągalne dla programów szpiegowskich instalowanych na komputerze ofiary). Ten sposób ataku jako tani i dostępny dla każdego wścibskiego użytkownika (nie wymaga specjalnych umiejętności) uznano za szczególnie niebezpieczny. Dalej rozważano zagrożenie takim właśnie atakiem – nie uwzględniając możliwości stosowania anten kierunkowych przez napastnika.

W laboratoriach firmy Siltech oraz WAT przeprowadzono szereg pomiarów i badań zmierzających do rozpoznania dla bezprzewodowych klawiatur co najmniej:

- widma tego promieniowania,
- zasięgu promieniowania urządzeń,
- przenikania sygnału przez przeszkody naturalne dla reprezentatywnych środowisk pracy.

Badania dotyczyły tylko warstwy fizycznej połączeń. Poddawano im różne klawiatury, uznane za rokujące sukces rynkowy i wyznaczające kierunek rozwoju, mieszczące się w rozsądnym przedziale cenowym. Czytelnikowi zainteresowanemu stroną techniczną badań i wynikami pomiarów można polecić opracowania [5] i [6]. Szczegółowe wyniki zawarto w pracy [7].

Zasięgi sygnału

Dalej przedstawiono wyniki wybranych badań zmierzające do określenia skutecznych zasięgów przechwytywania informacji. Rozpoznawano maksymalne odległości od klawiatur, z których możliwe było przechwytywanie sygnału czytelnego dla odpowiedniej stacji bazowej, bez dodatkowego wzmocnienia sygnału z anteny odbiorczej ani dodatkowych anten. Pomiarów zasięgu na potrzeby niniejszego opracowania dokonywano w następujących warunkach:

1. *Teren otwarty* – badanie przeprowadzono w terenie otwartym, płaskim bez żadnych przeszkód między nadajnikiem a odbiornikiem, z dala od powierzchni, które mogłyby odbijać sygnał.

2. *Dwoje drzwi* – badanie przeprowadzono w pomieszczeniach w amfiladzie, oddzielonych dwoma drzwiami osadzonymi w ściankach działowych; pierwsze to drzwi biurowe wykonane z płyty MDF o grubości 4 cm z oszkloną górną częścią, drugie to metalowe drzwi antywłamaniowe.

3. *Dwie ścianki i urządzenia* – badanie przeprowadzono w pomieszczeniach oddzielonych dwoma ścianami działowymi (zawierającymi także instalację elektroenergetyczną) zbudowanymi z czerwonej cegły, oklejonymi z obydwu stron płytą kartonowo-gipsową. Na drodze transmisji występowały typowe urządzenia AGD (lodówka, zamrażarka), pracujący odbiornik TV oraz pracujący komputer stacjonarny wyposażony w klawiaturę bezprzewodową Bluetooth.

4. *Klatka schodowa* – badanie przeprowadzono z klatki schodowej, pół kondygnacji poniżej pomieszczeń opisanych powyżej jako dwoje drzwi (pomieszczenia w amfiladzie, oddzielone dwoma drzwiami: biurowymi i metalowymi – antywłamaniowymi, osadzonymi w ściankach działowych).

5. *Dwie ściany suporeks* – badania przeprowadzono w pomieszczeniach biurowych oddzielonych dwoma ścianami działowymi wykonanymi z suporeksu o grubości 30 cm.

Dodatkowo wykonano próbę przechwycenia sygnału klawiatur radiowych umieszczonych w pomieszczeniu na trzecim piętrze budynku, za zamkniętymi drzwiami balkonowymi. Są to drzwi plastikowe, trzykomorowe posiadające podwójną szybę. Między szybami znajduje się próżnia (są to obecnie najbardziej typowe okna na rynku). Stanowisko przechwytujące zlokalizowano na zewnątrz budynku mieszkalnego w odległości poziomej 3,5 m do fasady balkonu i w odległości w pionie 9 m w dół. Próba zakończyła się powodzeniem.

Podczas badań przenikania fal radiowych dokonano pewnych obserwacji, których nie udało się uogólnić, ale wydaje się, że dobrze oddaje je kolokwialne sformułowanie jednego z uczestników opisanych wyżej działań: „Stropy zachowują się nieobliczalnie”.

2) Stan na 9 lipca 2007 r.

Wyniki w budynkach z nowego budownictwa były zbliżone i wskazywały na dobrą przenikalność ścian. W budynku głównym Wojskowej Akademii Technicznej ścianki działowe wykazywały nieco podobną przenikalność, natomiast ściany nośne stanowiły dla badanych fal radiowych nieprzebytą przeszkodę. Warto jednak zaznaczyć, że budynek ten został postawiony w latach pięćdziesiątych ubiegłego stulecia, jak głosi plotka – z wbudowaną odpornością na niedalekie wybuchy jądrowe.

Konkluzje

Podsłuch klawiatur bezprzewodowych stanowi realne zagrożenie poufności informacji. W większości przypadków wystarczy wejść w zasięg emisji klawiatury, niosąc teczkę z pracującym notebookiem (i z odpowiednią stacją bazową). Pozwala to zarejestrować wszystkie naciśnięcia klawiszy klawiatury podsłuchiwanego komputera. Koszt urządzeń do takiego ataku jest równy cenie klawiatury, nie wymaga również specjalnych kwalifikacji, dlatego ten rodzaj ataku był głównym rozpatrywanym w niniejszym opracowaniu zagrożeniem.

Typ klawiatury	Teren otwarty	Dwoje drzwi	Dwie ścianki i urządzenia	Klatka schodowa	Dwie ściany suporeks
PS2	28,4 m	19 m	19 m	17 m	20 m
USB	27,3 m	17 m	17 m	15 m	19 m
Bluetooth	39,0 m	29 m	29 m	24 m	15 m

Tab. 2. Wyniki badań zasięgu działania podsłuchu klawiatur bezprzewodowych

Najważniejszym parametrem określającym szanse sukcesu napastnika i obrońcy jest zasięg klawiatury, a dokładniej granice strefy, w której możliwy jest skuteczny podsłuch. Na podstawie przeprowadzonych do tej pory badań można zapewnić, że odległość 35 m zapewnia skuteczną ochronę przed podsłuchem (prowadzonym bez specjalnych anten kierunkowych). Napastnik, aby mieć pewność sukcesu, musi zbliżyć się z odbiornikiem na odległość 15 m do klawiatury. Do prezentowanych wyników badań należy jednak podchodzić z pewną ostrożnością – dotychczas przebadano tylko kilka egzemplarzy/typów klawiatur i na tej podstawie trudno jest formułować wnioski o stosowalności wyników dla innych typów urządzeń, a nawet o powtarzalności wyników dla innych egzemplarzy badanych typów.

Na szczęście można zalecić prostą metodykę tzw. strefowania, czyli wyznaczania granicy bezpiecznej strefy emisji dla stanowiska komputerowego wyposażonego w bezprzewodową klawiaturę. Należy:

1. Przygotować komputer przenośny.
2. Odłączyć stację bazową badanej klawiatury i przyłączyć ją do komputera przenośnego.
3. Przygotować plany/szkice otoczenia dla kondygnacji, na której znajduje się stanowisko komputerowe, oraz kondygnacji poniżej i powyżej.
4. Naładować baterie klawiatury oraz komputera przenośnego. Monitorować poziom baterii i powtarzać ładowanie (wymieniać baterie na naładowane), ilekroć poziom naładowania baterii komputera przenośnego opadnie poniżej 95%.
5. Na komputerze przenośnym uruchomić na przykład aplikację Notatnik.
6. Włączoną klawiaturę umieścić w miejscu pracy, następnie wcisnąć i zablokować klawisz H.
7. Poruszać się z komputerem wokół klawiatury, obserwując ekran i wyznaczając miejsca, w których zanika odbiór znaków z klawiatury. Oznaczyć te miejsca na planie kondygnacji.
8. Powtórzyć wyznaczanie tych granic na kondygnacji poniżej i powyżej (o ile istnieją).
9. Podobnie wyznaczyć granice strefy na zewnątrz budynku, przy otwartych oknach.

Takie postępowanie pozwoli na wyznaczenie strefy zagrożenia podsłuchem. Można zalecić przestrzeganie następujących reguł:

- dokonanie strefowania,
- zwiększenie wyznaczonej strefy o rozsądny margines bezpieczeństwa (ok. 20%),
- ograniczenie dostępu obcych do wyznaczonej strefy,
- powstrzymanie się od pisania czegokolwiek na klawiaturze, jeśli w pobliżu znajduje się obcy,
- wprowadzenie zakazu pozostawiania jakichkolwiek przedmiotów w strefie przez obcych.

Terminu „obcy" użyto dla określenia osoby, która nie powinna mieć dostępu do informacji przetwarzanych na komputerze.

Opisany w pierwszym akapicie niniejszego rozdziału sposób podsłuchiwania to najprostsza forma tego procederu, a strefa wyznaczona opisaną wyżej metodą dotyczy zagrożenia tylko takim podsłuchem. Tymczasem nie można wykluczyć zastosowania przez napastnika anten kierunkowych. Niniejsze opracowanie nie pozwala wnioskować o zasięgu tego rodzaju podsłuchów, z pewnością jednak będą one większe niż te, które przedstawiono w tab. 2.

Na szczególne podkreślenie zasługuje praktyczna niewykrywalność podsłuchu klawiatur radiowych (oczywiście poza przypadkami użycia środków ochrony fizycznej), co czyni z niego atrakcyjną technikę operacyjną.

Oczywiście rezygnacja ze stosowania klawiatur bezprzewodowych rozwiązuje większość opisanych wyżej problemów…

Dodatkowe ostrzeżenie

Zaprezentowane dotychczas konkluzje dotyczą podsłuchu sygnału transmitowanego między klawiaturą a stacją bazową. Z badań laboratoryjnych wyłania się jednak możliwość podsłuchu także innych sygnałów, niepożądanych, ale jednak generowanych z anten różnych urządzeń bezprzewodowych (nie tylko klawiatur komputerów). To sygnały nadawane z anteny ale przedostające się do układów nadawczych drogą przesłuchów (przez indukcję lub po liniach zasilania) wewnętrznych sygnałów z innych podzespołów elektronicznych komputera. **Można spodziewać się możliwości skutecznego podsłuchu każdego urządzenia z włączonym nadajnikiem**

sieci bezprzewodowej czy Bluetooth, i to podsłuchu na częstotliwościach poniżej 1 GHz.

Autorzy niniejszego opracowania są zdania, że teoretycznie podsłuch jest możliwy w przypadku wszelkich urządzeń elektronicznych, ale jeśli urządzenie zawiera włączony układ antenowy, to problem podsłuchu (i to wcale nie głównego transmitowanego sygnału) przesuwa się zdecydowanie z obszaru opowieści o żelaznym wilku w obszar realnych zagrożeń. Przyczyną jest pojawiająca się zupełnie nowa jakość – do tej pory emisja ujawniająca dotyczyła sygnałów niezwykle małej mocy, w rozważanych przypadkach (komputerów z antenami nadawczymi) emisja ujawniająca to sygnał zaledwie dziesięciokrotnie słabszy od głównego sygnału roboczego anteny.

Adam E. Patkowski
Robert Piotrowski

Literatura:

1. 802.15.1 IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). IEEE 14 June 2005.
2. Janczak J.: *Zakłócanie informacyjne,* Akademia Obrony Narodowej, Warszawa, 2001 r.
3. *Keyloggers*. [@]: *http://www.2-spyware.com/keyloggers-removal*, stan z dnia 10 czerwca 2007 r.
4. Kossowski R., Trela K.: *Emisja elektromagnetyczna sprzętu komputerowego jako zagrożenie bezpieczeństwa informacji*. II Krajowa Konferencja Zastosowań Kryptografii Enigma'98. Warszawa, 1998.
5. Patkowski A. E., Piotrowski R.: *Bezprzewodowe klawiatury – czy to bezpieczne?*, materiały XI Krajowej Konferencji Zastosowań Kryptografii Enigma 2007, Warszawa, 2007 r.
6. Patkowski A. E., Piotrowski R.: *Bezprzewodowe klawiatury – nowe możliwości podsłuchu*. X Seminarium Techniczne aspekty przestępczości teleinformatycznej. Wyższa Szkoła Policji, Szczytno, 2007.
7. Piotrowski R.: *Badanie zagrożeń dla bezpieczeństwa informacji wynikających z użytkowania bezprzewodowych urządzeń zewnętrznych,* praca magisterska, WAT, Warszawa, 2007.
8. Rozporządzenie Rady Ministrów z 29 czerwca 2005 r. w sprawie Krajowej Tablicy Przeznaczeń Częstotliwości.
9. Szczypiorski K., Cabaj K., Margasiński I. Kruszyński A.: *Rozwój sieci telekomunikacyjnych i sieci następnej generacji – aspekty strukturalne, funkcjonalne, techniczne i normalizacyjne.* Cześć III: *Analiza zagrożeń i ochrona danych w sieciach bezprzewodowych. Raport końcowy.* Warszawa, 2005 r.
10. *Windows Platform Design Notes. Designing Hardware for the Microsoft Windows Family of Operating Systems. Keyboard Scan Code Specification. Revision 1.3a*, Microsoft Corporation, March 16, 2000.
11. Zestawienia ofert klawiatur bezprzewodowych z portali www.skapiec.pl i www.ceneo.pl, stan na 9 lipca 2007 r.

Teoria ochrony informacji

(część 2.)

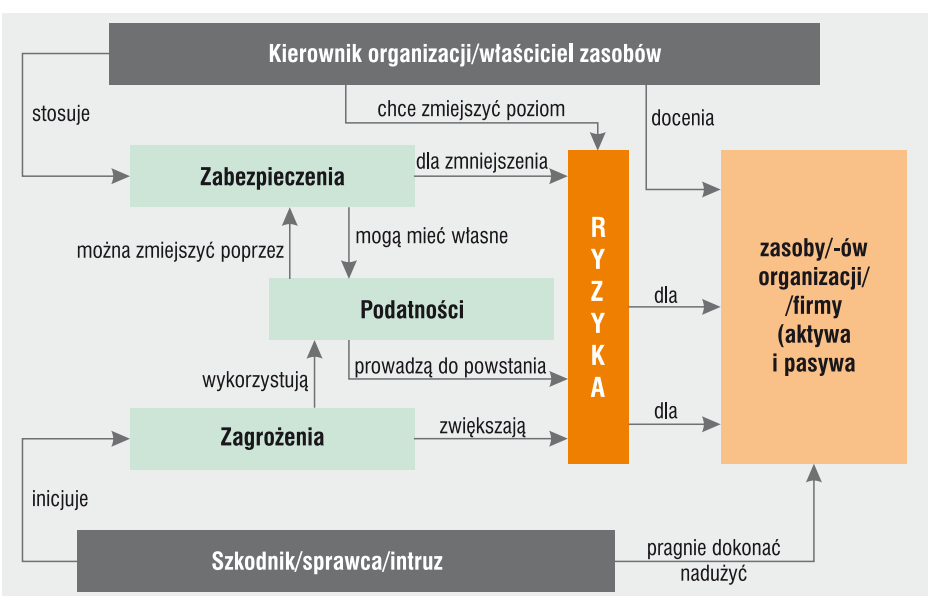
Ile (zgodnie z zaprezentowaną w wstępie do części I cyklu analizą funkcjonalną – AF), możemy powiedzieć, że po przedstawionej potrzebie ochrony informacji (etap 1. AF) oraz zrozumiałej dla menedżerów konieczności realizacji tego zadania w danych warunkach (etap 2. AF) już mamy pewien pogląd na problem ochrony informacji, o tyle dla pełnego rozwinięcia zapisu tego zjawiska w całej jego złożoności brak nam identyfikacji funkcji tej ochrony, jej celowość bowiem jest w środowisku biznesowym przez większość menedżerów (intuicyjnie) w pełni rozumiana

1. Wstęp

Spróbujmy zatem w ramach szerokiej analizy systemowej odpowiedzieć na pytanie, jakie są funkcje i cele końcowe (etap 3. AF) ochrony informacji, tylko na tej podstawie bowiem możemy „dopracować się" kilku dobrych idei (etap 5. AF), dających nam szansę na wybór teoretycznie quasi-optymalnego rozwiązania i jego wdrożenie w naszej firmie/korporacji/organizacji.

Dlaczego „quasi", a nie „rzeczywistego", czyli optymalnego w pełni? Dlatego, że zawsze i wszędzie tam, gdzie decyduje reguła obcinania kosztów, mamy sytuacje, w których pomija się sygnalne zagrożenia dotyczące istoty sprawy lub się ich nie docenia – a to już wyklucza istnienie tego rzeczywistego optimum. Mamy więc rozwiązanie optymalne, ale wyłącznie dla założonych (wprowadzonych i mniej lub bardziej świadomie określonych) ograniczających pełne widzenie problemu, warunków brzegowych. Nagminne jest bowiem ocenianie posiadanych zasobów wyłącznie od strony właścicielskiej i użytkowej pod względem biznesowym i operacyjnym. Bardzo często zaniedbuje się obowiązek archiwizacji i utylizacji już wykorzystanego zasobu. Nad wyraz rzadko analizuje się podjęte działania ochronne od strony potencjalnego intruza – przeciwnika, pragnącego dobrać się do naszych chronionych zasobów informacyjnych.

Spróbujmy zatem przyjrzeć się tym zjawiskom nieco bliżej. (Rys. 1.).



Rys. 1. Schemat oddziaływań na zasoby w firmie

2. Informacja jako wartość

Kiedy mówimy „informacja", zazwyczaj zakładamy, że nasz rozmówca rozumie przez to pojęcie to samo co my. Ale czy tak jest naprawdę...?

Sięgnijmy zatem do pojęć zdefiniowanych i ujętych w sposób normatywny[1]:

1. Informacja (w teorii informacji).

Wiedza redukująca lub usuwająca niepewność, dotycząca określonego zdarzenia z danego zbioru zdarzeń możliwych.

• PN-ISO/IEC 2382-16:2000 – 16.01.03 (wg stanu na 31.12.2005[1])

1) *Informatyka. Terminologia znormalizowana i wykaz norm,* wyd. PKN, Warszawa, 2006

2. Informacja (przetwarzanie informacji).

Wiedza dotycząca obiektów, takich jak fakty, pojęcia, przedmioty, zdarzenia i idee.

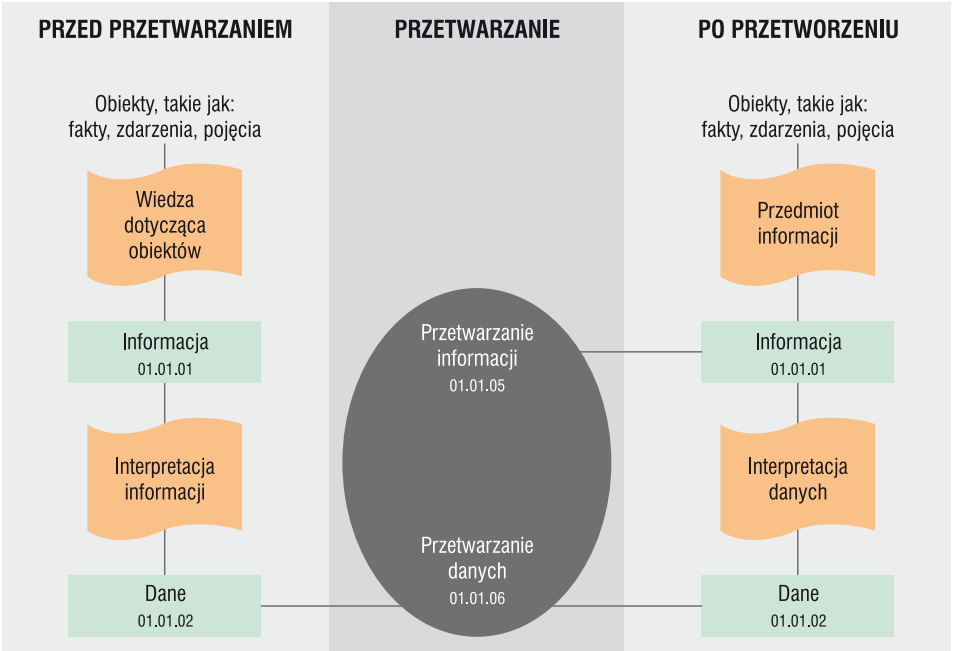
- PN-ISO 1087-2:2001 – 2.1 (wg stanu na 31.12.2005[1])

3. Informacja (w przetwarzaniu informacji).

Wiedza dotycząca obiektów, takich jak fakty, zdarzenia, przedmioty, procesy lub idee, zawierająca koncepcję, która w ustalonym kontekście ma określone znaczenie.

- PN-ISO/IEC 2382-1:1996 – 01.01.01;
- PN-N-01602:1997 – 2.71 (wg stanu na 31.12.2005[1]).

Kwestię normatywnie określonej relacji między informacją a danymi w procesie przetwarzania obrazuje rys. 2.



Rys. 2. Wzajemne relacje między informacją a danymi (ISO 2382-2: 1996), na podstawie: J. Krawiec BSO, PKN, Warszawa, 2005)

Łącznie w przywołanej publikacji terminologicznej[1] (s. 95–99) mamy udostępnione 38 definicji zaczynających się od słowa „informacja...” wraz ze wskazanymi, jednoznacznie je określającymi, odpowiednimi normami.

W praktyce biznesowej posiłkujemy się uogólnieniami, widzianymi w podstawowym łańcuchu skojarzeń, i są to:

- **informacja**, jako wiedza dotycząca faktów (obiektów analizy informacyjnej);
- **dane**, jako prezentacja informacji dowiązanej do faktu (często w postaci już zinterpretowanej na potrzeby danego biznesu – zob.: pakiet informacyjny);
- **pakiet informacyjny**, jako jednostkowe uporządkowane dane przedstawione w ujednoliconej postaci na nośniku informacyjnym (trwałym – *hard copy*[2] lub OEM[3] ew. ulotnym – transmisja z wykorzystaniem ICT[4]);
- **zbiór** – baza danych, jako połączenie informacji i danych zapisanych i dostępnych wg znanych i określonych jednoznacznie korelacji (np. MS ACCESS jako baza relacyjna itp.);
- **baza wiedzy** (jawnej i ukrytej), jako połączenie informacji i danych o określonych wcześniej atrybutach, możliwych do wyszukiwania i łączenia z wykorzystaniem predykatów i rachunku skojarzeń (np. baza ekspercka z danej dziedziny itd.).

Nie zawsze są one jednakowo interpretowane przez poszczególnych użytkowników – menedżerów biznesowych.

Chcąc ujednolicić zrozumienie (choćby hasłowe) pojęcia informacja, spróbujmy odnieść się do niego „z zewnątrz” poprzez identyfikację jego podstawowych atrybutów, tylko wtedy możemy nie tylko dokończyć opis informacji, ale również prowadzić wszelkie dalsze, niezbędne dla kolejnych przemyśleń teoretycznych i praktycznych – analizy formalne i skojarzeniowe.

2.1. Atrybuty informacji

Przeglądając dokumenty ustawowe (OIN, ODO), normy (PN, EN, ISO/IEC), standardy sojusznicze (STANAG's; AP's) oraz zalecenia biznesowe (OECD) i stowarzyszeniowe (ISACA) związane z ochroną informacji, spotykamy się z wyszczególnieniem od kilku do kilkunastu atrybutów przypisanych hasłu informacja, zależnie od wskazanego (określonego w danym dokumencie) przewidywanego środowiska funkcjonowania ochrony tych atrybutów.

Charakterystyczne dla opisu informacji są przede wszystkim (powtarzające się) trzy z nich (PID/CIA):

- poufność (ang. *Confidentiality*),
- integralność (ang. *Integrity*),
- dostępność (ang. *Availability*)

oraz występujące w ponad połowie analizowanych dokumentów (prawie identycznie identyfikowane i opisywane) kolejne cztery atrybuty (RANN/AAUR):

- rozliczalność (ang. *Accountability*),
- autentyczność (ang. *Autenticity*),
- niezaprzeczalność (ang. *Undeniability, Unquestionability*),
- niezawodność (ang. *Reliability*),

przy czym te ostatnie odnoszone są nie tylko do samej informacji, ale wykorzystywane są również jako atrybuty zbiorów danych oraz sprzętu i oprogramowania w systemach informacyjnych i informatycznych.

W każdym przypadku ocena bezpieczeństwa informacji oparta jest na możliwości zapewnienia, osiągnięcia i utrzymania na założonym poziomie wszystkich jej zdefiniowanych atrybutów (niezwykle istotne jest w tym przypadku odniesienie się do zdarzeń incydentalnych zagrażających samej informacji – co identyfikuje szerzej protokół ISO/IEC TR 18044 Security Incident Management).

Podstawowym dokumentem opisowym zarządzania bezpieczeństwem informacji jest międzynarodowa norma

2) *hard copy* – trwały mechanicznie nośnik informacyjny czytelny bezpośrednio dla człowieka, dokument papierowy, fotografia, plan, mapa itp.

3) OEM – trwały mechanicznie nośnik informacyjny czytelny pośrednio dla człowieka, zapisany z użyciem technik optycznych (pamięć holograficzna, CD), elektronicznych (pamięci EPROM itp.) lub magnetycznych (pamięć taśmowa – streamer, HDD/FDD itp.)

4) ICT – *Information&Communication Technology*, technologia przesyłu bezpośredniego (tunelowego) lub pakietowego, kodowanego lub szyfrowanego pliku informacyjnego (Internet, e-mail, faks, teleks, SMS itp.)

ISO/IEC 27002:2007, tożsama tekstowo z drugą edycją normy ISO/IEC 17799:2005 (opracowana w KT 182 PKN, jest dostępna w języku polskim jako PN-ISO/IEC 17799:2007), jej część definicyjna zawiera zapisy ujednolicone z ISO/IEC 13335-1:2004 (2. ed.) oraz z ISO/IEC Guide 73:2002, których treść została odpowiednio przeniesiona do specyfikacji wymagań dla systemu zarządzania bezpieczeństwem informacji – normy ISO/IEC 27001:2005 (polska edycja PN-ISO/IEC 27001:2007).

Zarządzanie bezpieczeństwem informacji jest możliwe wyłącznie w określonym i ograniczonym obszarze objętym systemem informacyjnym obejmującym informacje, nośniki, urządzenia i użytkowników informacji.

Prawidłowo skonstruowany system informacyjny powinien bez względu na postać (bezpośrednia/zapis na nośniku) i charakter informacji (jawna, chroniona/niejawna) spełniać trzy podstawowe kryteria:

I. Zapewniać bezpieczeństwo informacji.

II. Zapewniać bezpieczeństwo świadczenia usług.

III. Zapewniać autentyczność i rozliczalność danych i podmiotów.

Każde z przedstawionych powyżej kryteriów można i trzeba scharakteryzować:

I. Kryterium I składa się z głównych elementów:
- **poufność informacji** (ang. *Information Confidentiality*) – co oznacza, że informacje są dostępne tylko i wyłącznie dla osób, które są do tego uprawnione;
- **nienaruszalność/integralność informacji** (ang. *Information Integrity*) – co oznacza zagwarantowanie dokładności i kompletności informacji oraz metod i sposobów ich przetwarzania;
- **dostępność informacji** (ang. *Information Availability*) – co oznacza zapewnienie, że upoważnieni (autoryzowani) użytkownicy mają dostęp do informacji i związanych z nimi zasobów zawsze wtedy, gdy jest to wymagane.

II. Kryterium II – składa się z głównych elementów:
- **niezawodność systemu** (ang. *System Reliability*) – co oznacza, że na systemie można polegać bezwzględnie, jest on przyjazny i odporny na błędy przypadkowe operatora (*fool proof*);
- **nienaruszalność/integralność systemu** (ang. *System Integrity*) – co oznacza dokładność systemu oraz użytych w nim metod i sposobów przetwarzania informacji;
- **dostępność systemu** (ang. *System Availability*) – co oznacza zapewnienie, że upoważnieni (autoryzowani) użytkownicy mają gwarantowany dostęp do systemu oraz jego zasobów.

III. Kryterium III – składa się z głównych elementów:
- **autentyczność danych** (ang. *Data Indisputable*) – co oznacza, że dane przechowywane w systemie i udostępniane są pewne i można na nich polegać;
- **autentyczność podmiotów** (ang. *Indisputable of Subjects*) – co oznacza dokładność identyfikacji podmiotu korzystającego z systemu oraz potwierdzenie uprawnień do użytkowania zgromadzonych w nim informacji;
- **rozliczalność podmiotów** (ang. *Settlement Accounts of Subjects*) – co oznacza zapewnienie, że upoważnieni (autoryzowani) użytkownicy nie mają możliwości zanegowania faktu swego dostępu do systemu i udokumentowanego korzystania jego zasobów;

Dopiero dla systemu informacyjnego tak skonstruowanego, aby poprzez posiadanie i określenie każdego z elementów spełniał ww. kryteria, możemy przystąpić, w kolejnych krokach, wykorzystując dorobek i doświadczenie z praktyki stosowania zasad kodeksowych brytyjskiej, a obecnie już międzynarodowej normy (rys. 7 w cz. 1. artykułu – *Zabezpieczenia 3/2007*), do kolejnych czynności normatywnych związanych z SZBI/ISMS, czyli do:
- analizy zagrożeń oraz oceny stopnia i poziomu występujących dla informacji ryzyk;
- konstruowania polityki bezpieczeństwa informacji stanowiącej wykładnię zasad zarządzania informacją w tym systemie;
- wdrażania metod i sposobów niwelujących podatności na przewidywane oraz prawdopodobne zagrożenia zarówno samej informacji, jak i nośników ją zawierających.

2.2. Podatności informacji i jej nośników

W trakcie dalszych prac analitycznych wypada odpowiedzieć na (skądinąd) zasadnicze pytania: Co, jak, kiedy i na ile zagraża analizowanej przez nas informacji, oraz jak wygląda jej podatność na skutki zmaterializowania się tych przewidywanych czy też rzeczywistych zagrożeń.

W procesie ochrony informacji o wszystkich tych zjawiskach mówimy w dwóch współzależnych obszarach:
- jako podatnościach w odniesieniu do tzw. surowej postaci informacji;
- jako celowych zagrożeniach (niebezpieczeństwach) dla każdej postaci informacji, w tym także skojarzonej bezpośrednio z jej nośnikiem (papier, CD, *pen drive* itp.).

2.2.1 Co rozumiemy przez podatności surowej postaci informacji

Na ogół wszelkie zaburzenia i zmiany zachodzące w przekazie informacyjnym (lub w tzw. przekazie mimowolnym), do których zaliczamy:
- zwykłą postać ulotną informacji (np.: tekst rozmowy bezpośredniej lub telefonicznej/radiowej niezapisany w żadnej dostępnej formie na dowolnym nośniku trwałym) przekazywaną w układzie „nadawca" – „bezpośredni odbiorca", która jest podatna na zakłócenia przypadkowe lub celowe bez możliwości odtworzenia treści pierwotnej informacji [bardzo często odbiorca mimowolnie uzupełnia braki wynikłe w trakcie przekazu (w sposób dla niego naturalny) i „da się pokroić na plasterki", że to właśnie taką informację w tej rozmowie usłyszał oraz zapamiętał (trudno tu mówić o złej woli czy też celowej konfabulacji)];
- niechronioną postać ulotną informacji w systemach informacyjnych lub informatycznych (bardzo podatną na przypadkowe lub celowe zniekształcenia) przekazywaną w układzie „nadawca" – „punkt składowania informacji odbiorcy/adresata przekazywanej informacji", która jest podatna na zakłócenia przypadkowe lub celowe pozorujące formę treści pierwotnej informacji oraz ułatwia manipulację (opóźnienie, modyfikowanie, okresowe zagubienie lub wręcz zniszczenie);
- przypadkową generację (czytelną dla osób postronnych) części lub całości informacji w okolicznościach nieformalnych lub celowo sprowokowanych w odniesieniu do właściciela informacji lub jej czasowego posiadacza.

2.2.2 Co rozumiemy przez podatności nośników informacji

Głównie brak nadzoru nad samymi nośnikami (łatwy dostęp nieupoważnionych osób trzecich do treści zapisu) oraz niedostateczne zabezpieczenia nośników i urządzeń przechowujących informacje (możliwość kopiowania całości nośników oraz ich treści bez pozostawienia śladów).

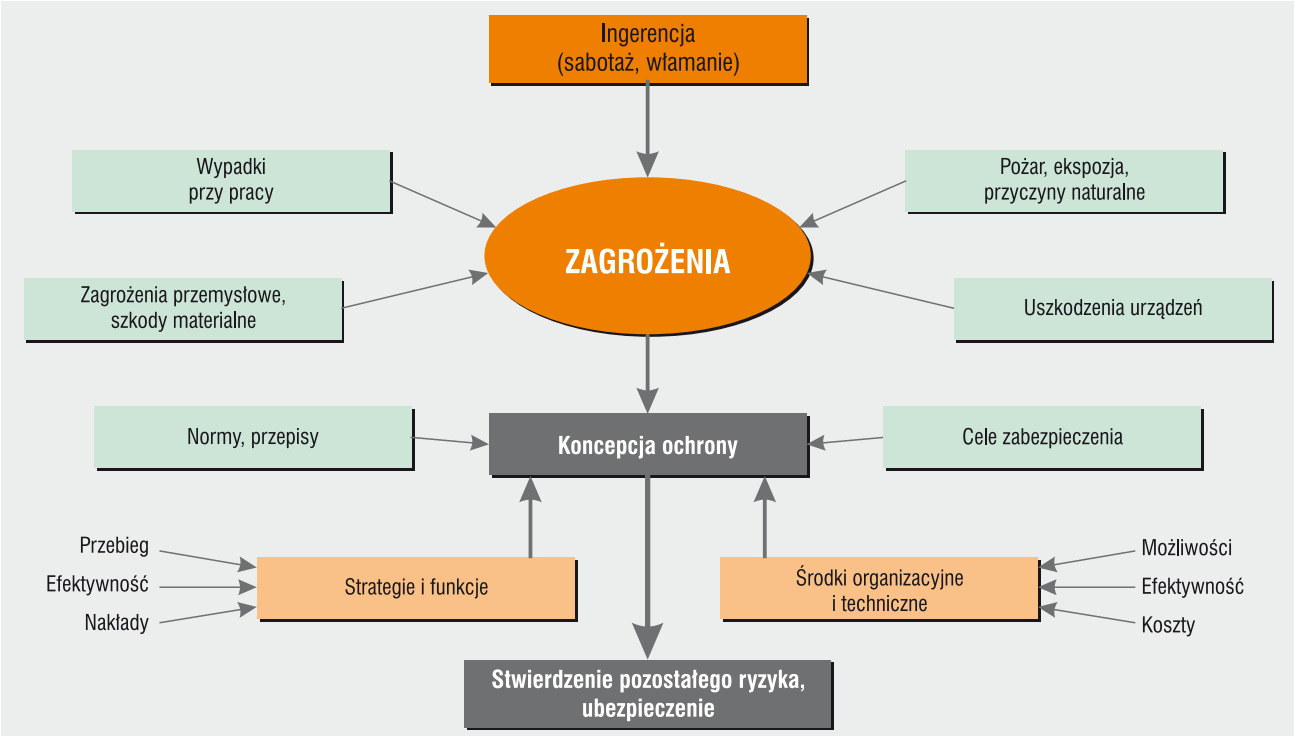
Specyficzną podatnością jest n-krotność rozpowszechnianej informacji pozwalająca na jej cząstkowe lub całościowe odtworzenie w trybie analizy mozaikowej danych podstawowych[5].

3. Niebezpieczeństwa grożące „informacji”

Ujęcie w cudzysłów wyrazu informacja wiąże się z jego szerokim, popularnym i pozadefinicyjnym rozumieniem, jako „pojęcia – worka”, w którym to każdy z dyskutantów znajdzie coś dla siebie, co będzie pasowało do wygłaszanych przezeń opinii.

nego w niniejszym artykule. Ponadto w praktyce ochrony informacji nad wyraz często spotkać się można z oczekiwaniami i żądaniami menedżerów biznesu (skierowanymi pod adresem konsultantów i audytorów) zamykającymi się w haśle „Zróbcie mi to PBI (politykę bezpieczeństwa informacji), bo nie będę (nie chcę być) gorszy od innych”.

Ma się to niestety nijak do teorii zjawiska – bo co prawda są zdefiniowane podstawowe uniwersalne zasady polityki bezpieczeństwa pasujące do każdej firmy, ale... aby stworzyć łańcuch bezpieczeństwa i zamknąć w nim obszar chroniony, musimy wiedzieć:



Rys. 3. Zasadnicze zależności budowy koncepcji ochrony[6]

Teoria ochrony informacji proponuje posiłkowanie się w tym przypadku określeniem system informacyjny z jego zasobem informacyjnym (czyli system, w którym możemy odnaleźć wszystkie elementy łańcucha skojarzeniowego związanego z ogólną definicją pojęcia informacja – wszystkie, bo wiemy że nie da się połączyć w całość brakujących ogniw).

Dla tak ogólnie rozumianego „zasobu/-ów” firmy (rys. 1., cz. II) można próbować opracować koncepcję ochrony, choć jest to zadanie trudne, bo większość menedżerów procesów biznesowych postrzega zagrożenia dla tych zasobów wyłącznie jako sabotaż i ingerencję z zewnątrz firmy. A jak o tym wypowiada się ogólna teoria ochrony? (rys. 3.)

Niezbyt często można spotkać się z tak szerokim i analitycznym podejściem do tej kwestii, jakże istotnej dla całościowego analizowania problemu ochrony informacji.

Patrzenie przez pryzmat działań biznesowych nie zawsze poszerza optykę widzenia zasadniczego problemu opisywa-

- co chronimy, czyli jakie są zasoby i struktura chronionego systemu informacyjnego;
- przed czym chronimy, czyli jakie są zagrożenia, oraz jaki model jest odpowiedni do oceny ryzyka dla naszego systemu informacyjnego oraz objętego nim (generowanego, przetwarzanego, udostępnianego, archiwizowanego i ramach niego utylizowanego) zasobu informacji.

3.1. Metody projektowania zabezpieczeń dla systemu informacyjnego z jego zasobem

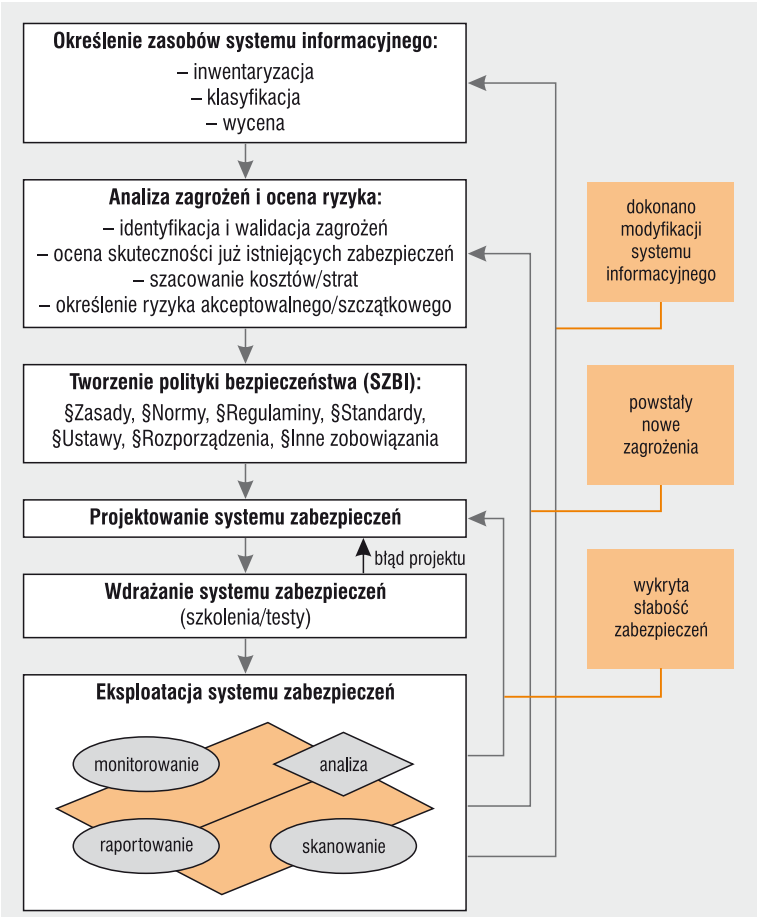
Metody te wynikają bezpośrednio z analizy systemowej (rys. 4., cz. I) oraz wymagań ochrony (rys. 6., cz. I), a u ich podstaw leży jedna zasadnicza myśl – nawet najlepsze systemy zabezpieczeń mają swój ograniczony technicznie i technologicznie cykl życia, ponadto przygotowane i uruchomione przez specjalistów, muszą być nadzorowane przez użytkownika we wszystkich aspektach ich późniejszego działania. To w trakcie prawidłowej eksploatacji (analiza stanu – skanowanie – raportowanie – monitorowanie zmian – analiza stanu) wykrywamy słabości zabezpieczeń oraz identyfikujemy nowe zagrożenia. Ponadto niezbędne jest uwzględnianie wszelkich modyfikacji wprowadzanych w samym chronionym systemie[7].

5) Analiza mozaikowa – system odczytu nakładkowego informacji cząstkowych stosowany pierwotnie przez wywiad japoński przed II wojną światową, konkurencyjny dla tzw. wywiadu białego; łączył wszystkie dostępne jawne i ukryte źródła informacyjne związane, choćby pośrednio, z analizowanym problemem.

6) A. Wójcik, Materiały szkoleniowe Podyplomowego Studium Ochrony Informacji, Katowice, 2004.

7) M. Stawowski, K. Rokita: *Bezpieczeństwo informacji od A do Z*, Wiedza i Praktyka, Warszawa, 2003.

Podstawę do kwalifikowania przydatności użytej metody stanowią ujęte w cykl:
– określenie zasobów;
– analiza zagrożeń i ocena ryzyka;
– przyjęta polityka bezpieczeństwa informacji;



Rys. 4. Przykładowy cykl życia systemu zabezpieczeń

– sposób jej wdrożenia;
– łatwość i skuteczność eksploatowania wdrożonych zabezpieczeń,

co przedstawia rys. 4.

3.2. Zasady projektowania zabezpieczeń dla systemu informacyjnego z jego zasobem

Podstawę projektowania zabezpieczeń stanowi odwzorowanie zasobów systemu informacyjnego, zwane bardzo często mapą zasobów i wartości.

Stworzenie samej mapy zasobów wymaga:
– ustalenia grup i kategorii użytkowników poszczególnych informacji – pakietów informacyjnych – zbiorów itd., przy zachowaniu odpowiedniego oszacowania i znaczenia ich funkcjonowania dla działalności firmy;
– ustalenia zadań realizowanych przez system informacyjny (jego podsystemy w układzie wagowym i hierarchicznym) dla działalności firmy;
– ustalenia zasobów (informacyjnych, fizycznych, technicznych, osobowych) i ich wykorzystania w korelacji do grup i zadań systemu informacyjnego.

Oszacowanie wartości zasobów wymaga:
– w odniesieniu do informacji – ocenienia skutków (kosztów) ich ujawnienia, niepożądanej modyfikacji, niedostępności lub wręcz zniszczenia;
– w odniesieniu do zasobów fizycznych i technicznych będą to przypuszczalne koszty naprawy lub wymiany elementów albo całych urządzeń;
– w odniesieniu do zasobów osobowych będą to koszty zaburzeń organizacyjnych lub szacunkowe koszty utraty image'u firmy i pozycji na rynku[8].

Do kosztów dolicza się szacunki i wyceny związane z samym systemem zabezpieczeń (obliczone względem założonego poziomu szczelności, niezawodności i wydajności) przy uwzględnieniu posiadanej i przewidywanej do nabycia technologii wraz z kosztami jej implementacji (szkolenia, nakład pracy na wdrożenie i eksploatację). Prezentowane podejście wynika z zasad sporządzania bilansu rocznego (identyfikowalne aktywa i pasywa firmy).

W niektórych starszych opracowaniach z zakresu securitologii oraz zarządzania bezpieczeństwem (do roku 1999) można spotkać się z określeniem „wymagania funkcjonalno-techniczne zabezpieczeń", które jest tożsame z wyżej przedstawionymi.

Wówczas obowiązywały i obecnie obowiązują uniwersalne zasady ochronne, zwane aktualnie zasadami PBI systemu informacyjnego, a stanowiące w swojej treści „podstawę" postępowania w obszarze chronionym[9]:

1. Zasada przywilejów koniecznych – każdy użytkownik systemu informacyjnego i jego zasobu posiada prawa ograniczone wyłącznie do tych, które są niezbędne i konieczne do wykonywania powierzonych mu zadań.

2. Zasada usług koniecznych – zakres dostępnych usług w ramach systemu jest ograniczony tylko do tych, które są konieczne do prawidłowego funkcjonowania firmy.

3. Zasada ubezpieczania zabezpieczeń – konieczne jest stosowanie wielowarstwowych zabezpieczeń, które ubezpieczają się wzajemnie (tzw. krotność przekrycia).

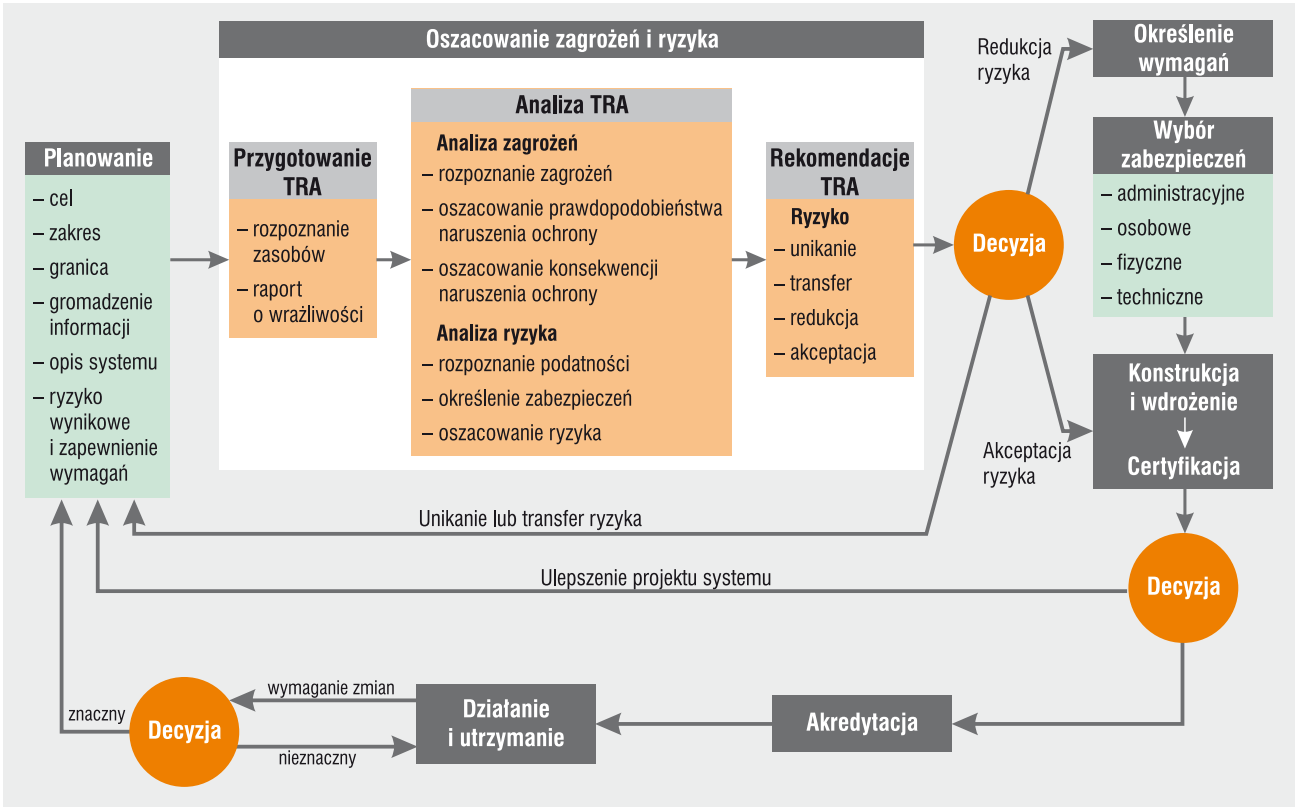
4. Zasada odpowiedzialności – za utrzymywanie właściwego poziomu bezpieczeństwa poszczególnych elementów systemu informacyjnego i jego zasobu odpowiadają konkretne osoby, które mają świadomość tego, za co są odpowiedzialne i jakie konsekwencje poniosą, jeżeli zaniedbają swoje obowiązki.

5. Zasada świadomości – wszyscy użytkownicy systemu informacyjnego wraz z jego zasobem są świadomi konieczności ochrony systemu i wykorzystywanych zasobów. Bezpieczeństwo systemu zależy w dużej mierze od bezpośredniego świadomego zaangażowania każdego pracownika organizacji.

6. Zasada najsłabszego ogniwa – poziom bezpieczeństwa systemu informacyjnego wyznacza najsłabszy (najmniej zabezpieczony) element tego systemu.

W tym ostatnim przypadku należy pamiętać, że ochrona wartościowych zasobów systemu nie może się opierać wyłącznie na jednym mechanizmie zabezpieczenia, nawet jeżeli zastosowano metody, techniki i technologie wysoce zaawansowane i o bardzo wysokim stopniu niezawodności, przypadkowa awaria bowiem pozostawia system bez ochrony.

8) M. Blim: *Zarządzanie jakością i bezpieczeństwem systemów TI*, materiały szkoleniowe IOP PW, Warszawa, 2004.
9) tamże.



Rys. 5. Model zarządzania ryzykiem

Projektowany system zabezpieczeń musi zatem uwzględniać wszystkie ww. uwagi i zasady.

3.3. Zasady postępowania przy analizie ryzyka dla systemu informacyjnego

Przeprowadzenie analizy ryzyka dla systemu informacyjnego wiąże się z koniecznością wyeliminowania wielu stereotypowych odniesień biznesowych, na ogół pomijających uwarunkowania kryzysowe i nadzwyczajne wynikające z obowiązującego ustawodawstwa polskiego. Dodatkowo należy zwrócić uwagę na elementy planowania ciągłości działania i odtwarzania po awarii (BCP/DRP – od ang.: *Business Continuity Plan/Disaster Recovery Planing*) oraz zarządzanie ciągłością działania (BCM – od ang.: *Business Continuity Management*) w rozległych strukturach systemów informacyjnych.

Podstawę do analizy stanowią rozwiązania modelowe (w tym ujęte w normach, rozwiązaniach resortowych i stowarzyszeniowych) ze szczególnym wskazaniem na wieloletnie doświadczenia sektora bankowego[10].

Chcąc mówić o zarządzaniu ryzykiem, należy zdawać sobie sprawę z dwu odrębnych ciągów:

– ciągu zdarzeń (incydent–zakłócenie–zagrożenie–ryzyko–materializacja ryzyka–koszty);
– ciągu procesów informacyjnych towarzyszących ww. zdarzeniom.

Rozwiązania normatywne (ISO 27001:2005) wręcz wymagają ustanowienia planów postępowania z ryzykiem stosownie do efektów jego analizy i oceny (akceptowalne lub nie do zaakceptowania; dopuszczalne lub niedopuszczalne; pomijane lub usuwane poza zakres działań firmy).

Warto zatem przywołać dobre praktyki z sektora bankowego, gdyż jest on miejscem ponoszenia skalkulowanego (i zarazem eliminowania zbędnego) ryzyka operacyjnego funkcjonowania na rynku usług i informacji finansowych. To właśnie w ramach protokołów normatywnych (ISO TR 13569 *Guidelines for the Management of IT Security*) opracowano model zarządzania ryzykiem na potrzeby systemów bankowych, przedstawiony na rys. 5.

Bank jest bowiem miejscem stałego i konsekwentnego analizowania każdej z wielu postaci ryzyka, do którego zalicza się:

a) **ryzyko technologiczne i techniczne** – związane ze stosowaniem nieadekwatnej, zawodnej lub źle wdrożonej technologii lub nieodpowiednim działaniem systemów biurowych i teleinformatycznych, adekwatnością sprzętu (hardware) i oprogramowania (software) do rodzaju i skali prowadzonej działalności, działaniem urządzeń telekomunikacyjnych, dostawami kluczowych usług (w tym telekomunikacja, energia elektryczna ze źródeł podstawowych i rezerwowych);

b) **ryzyko oszustw lub błędów wewnętrznych** – związane z np. oszustwami księgowymi, różnego rodzaju kradzieżami dokonywanymi przez pracowników, wykorzystywaniem informacji poufnych, nadużyciami w zakresie wykonywania czynności formalnych w imieniu i na rachunek banku/firmy/organizacji;

c) **ryzyko oszustw zewnętrznych** – związane z np. przestępstwami komputerowymi, malwersacjami, kradzieżami (energii, informacji, innych wartości) na niekorzyść i na rachunek banku/firmy/organizacji;

d) **ryzyko kadrowe** – związane ze stosowaniem nieefektywnych mechanizmów rekrutacji, szkolenia, oceny i motywowania pracowników, powodujących nieadekwatność kadry do rodzaju i skali prowadzonej działalności lub niepożądaną jej fluktuację oraz brak identyfikacji z bankiem/firmą/organizacją;

e) **ryzyko działalności operacyjnej** – związane np. z niewłaściwym przygotowaniem nowych transakcji i umów, problemami klientów z informacjami i danymi, niewłaściwą obsługą klientów, nieprawidłowo ustalanymi limitami wewnętrznymi,

10) M. Blim, M. Byczkowski, J. Zawiła-Niedźwiecki: *Zarządzanie ryzykiem operacyjnym w świetle wymogów Komitetu Bazylejskiego*, materiały konferencyjne XVI Szkoły Górskiej PTI, Szczyrk, 2004.

błędami proceduralnymi (np. złe opracowanie kontraktu, niewłaściwe przednegocjacyjne prognozy cen);

f) **ryzyko księgowe** – związane np. z ewidencjonowaniem transakcji w sprzeczności z przyjętymi w banku/firmie/organizacji zasadami rachunkowości lub nieprawidłowym przeksięgowaniem (szczególnie wobec klientów handlowych);

g) **ryzyko finansowe** – związane rynkiem walut (w tym z rynkiem bilansującym) oraz z regulacjami zewnętrznymi (transakcje giełdowe, sprzedaż usług) oraz niepełną kompensacją kosztów;

h) **ryzyko transakcyjne** – związane np. z rodzajem lub wielkością transakcji (lekceważenie opcji odbiorcy), niewłaściwą dokumentacją, nieuzasadnioną kompensacją sprzedaży, błędną realizacją transakcji (np. niewłaściwe negocjowanie), brakiem optymalizacji systemowej w odniesieniu do portfolia kontraktów i transakcji giełdowych;

i) **ryzyko prawne** – związane np. z brakiem odpowiednich regulacji, błędnymi regulacjami wewnętrznymi, błędami prawnymi w zawieranych umowach, potencjalnymi zmianami w przepisach, brakiem stabilności otoczenia regulacyjnego, niekorzystnymi rozstrzygnięciami w procesach sądowych;

j) **ryzyko funkcjonowania organizacji** – związane np. z nieprzestrzeganiem zasad BHP, funkcjonowaniem związków zawodowych i organizacji pracowniczych, relacjami z klientami, akcjonariuszami i osobami trzecimi (np. skargi i pozwy sądowe, informacje prasowe), nieadekwatną informacją zarządczą, niewłaściwym planowaniem, przestarzałymi mechanizmami zarządzania, niedostosowaniem struktury organizacyjnej do skali działalności banku/firmy/organizacji;

k) **ryzyko materialne i losowe** – związane z np. utratą wartości majątku, terroryzmem, wandalizmem (fizyczne zniszczenie zasobów), kataklizmami;

l) **ryzyko związane ze zleceniem czynności na zewnątrz** – związane z korzystaniem z usług podmiotów trzecich (*outsourcing*).

Odpowiednia identyfikacja i zarządzanie ryzykiem oraz adekwatne mechanizmy kontroli mogą nie tylko uchronić bank/firmę/organizację przed stratą, ale w efekcie – obniżyć koszty i zapewnić bardziej niezawodne bieżące działanie.

Świadomość wartości posiadanych aktywów w połączeniu z wiedzą o zagrożeniach i potencjalnych skutkach zmaterializowania się poszczególnych zagrożeń jest czynnikiem decydującym w procesach modyfikowania struktury banku/firmy/organizacji mających nie tylko zapewnić bezpieczeństwo informacyjne, ale zwiększyć bezpieczeństwo systemowe organizacji.

Jak to rozumieć, skoro mamy sytuację, w której na podstawie mniej lub bardziej trafnych ocen przyjętych dla incydentu czy też zakłócenia powinno się przyporządkować skutki ujawnionego zagrożenia, a w konsekwencji określić samo ryzyko oraz koszty jego materializacji (eliminacji lub maksymalnego ograniczenia wszelkich negatywnych skutków). Całość prac musi być bezwzględnie realizowana w myśl przepisów prawnych i technicznych, z zachowaniem wymogów ciągłości i poprawności działań.

Rzeczywista ocena występującego ryzyka jest zawsze bardzo trudna, nie ma bowiem dwu identycznych firm. Niemniej jednak stosuje się z powodzeniem grupy analiz zagadnień szczegółowych charakterystycznych dla poszczególnych systemów informacyjnych (bankowość, aeronautyka, medycyna, przemysł chemiczny i samochodowy itp.)[11].

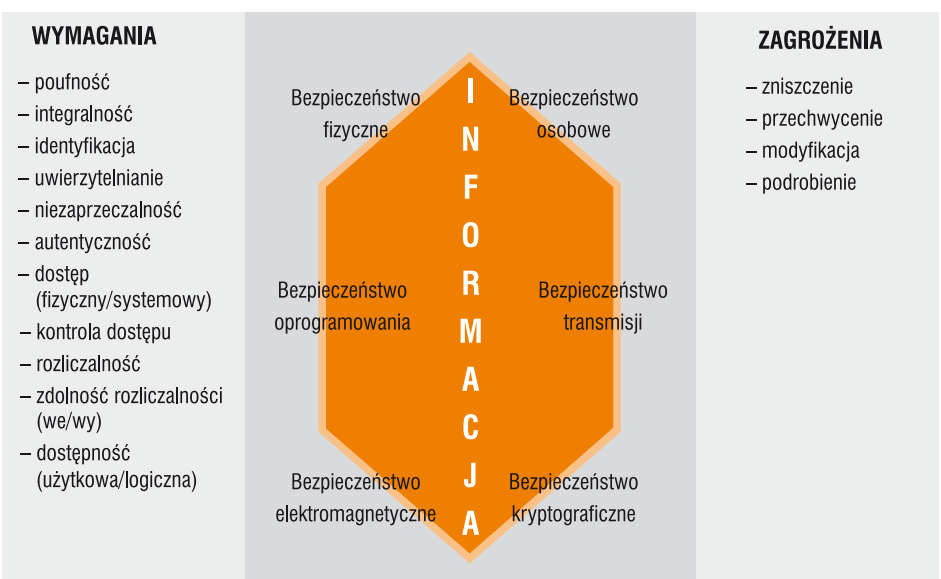
3.4. Kwalifikacja i kwantyfikacja ryzyk – rozwiązania programowane

W odniesieniu do systemów ICT (*Information&Communication Technology*), czyli informatycznych i telekomunikacyjnych powiązanych z sieciami i systemami rozległymi, opracowano zautomatyzowane systemy analizy ryzyka (głównie na potrzeby instytucji rządowych i dużych korporacji):

1. CRAMM (*CCTA Risk Analysis & Management Methodology*) – Wlk. Brytania, pakiet trzech części (identyfikacja i ocena podatności: 1–10 pkt; szacowanie ryzyka wg grup zagrożeń: 1–5 pkt; zbiór proponowanych/zalecanych rozwiązań – wg oceny pkt).

2. VIR'94 (*Voorschrft Informatiebeyeiliging Rijkdienst*) – Holandia, pakiet z sześciu części, w tym metoda D&V (5- i 3-etapowa analiza uzależnienia organizacji od ICT z jej podatnościami).

3. MARION – Wlk. Brytania, pakiet analizy kwalifikacyjno-kwantyfikacyjnej na potrzeby biznesu realizowany z wykorzystaniem znanych incydentów bezpieczeństwa w 27 kategoriach zasobów i zagrożeń (specjalizowany na podstawie prawa brytyjskiego).

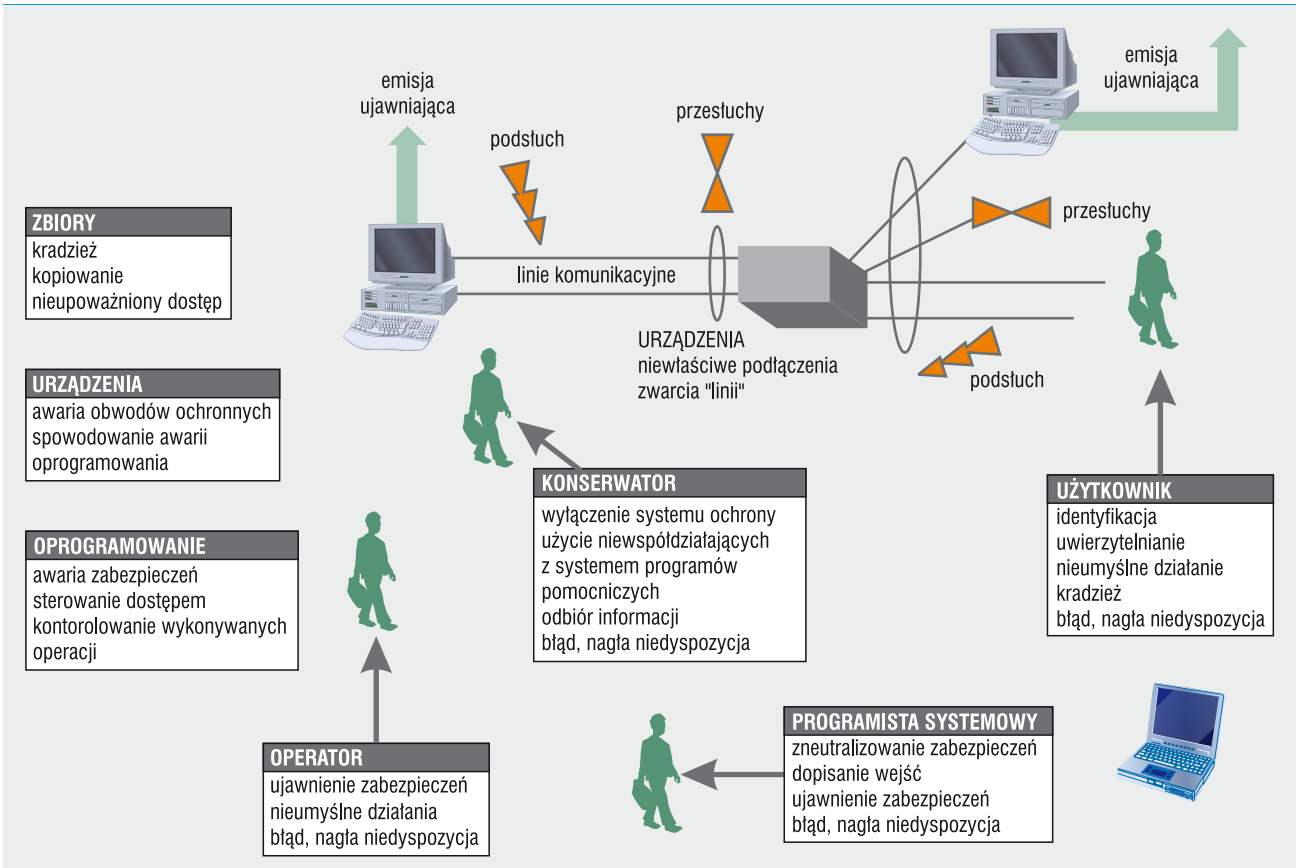


Rys. 6. Bezpieczeństwo informacji w STI

4. MAGERIT (*Methodology of Risk Analysisi&Management of Information Systems of Public Administration*) – Hiszpania, pakiet w trzech modułach i różnych proponowanych wersjach (C3) z odniesieniem do ICT w zakresie poziomu administracji użytkującej.

5. MASSIA (*Methode d'Audit de la Securite des Systems d'Information de l'Armement*) – Francja, pakiet wraz z oprogramowaniem narzędziowym dla sprawdzania SWB (szczególnych wymagań bezpieczeństwa) wg założeń ITSEC.

11) *Wybrane aspekty zarządzania wiedzą w przedsiębiorstwach UE*, pod red. T. Krupy, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, Opole, 2006.



Rys. 7. Bezpieczeństwo systemu informacyjnego

6. IST/RAMP (*International Security Technology/Risk Analysis Management*) – USA, program na sprzęt typu mainframe (komputery o dużej wydajności przetwarzania danych, których celem jest świadczenie usług dużej liczbie użytkowników) wykorzystujący metodologię kwantyfikacyjną dla systemów rozległych (pięć grup aktywów i odpowiadających im zagrożeń). Wyniki obrazowane są tabelarycznie na wydzielonym terminalu – PC jako stacja graficzna.

7. RISKPAC – USA, pakiet analizy kwalifikacyjno-kwantyfikacyjnej na potrzeby agencji rządowych (cztery kategorie instytucjonalne ICT, oddzielne zbiory aktywów i zagrożeń, możliwa korelacja wtórna i dodatkowa korekcja – oddzielny moduł zaleceń szczegółowych – wszystko na podstawie prawa amerykańskiego).

8. Pakiet BI/SAS+SAP – Polska, pakiet analizy ryzyka przemysłowego przedstawiony na SAS Forum 2005 jako wsparcie analityczne systemów ERP (baza zagrożeń jest rozwijana w trakcie wdrażania na podstawie badań ankietowych w firmie/baza aktywów ograniczona jest w swej treści do zawartości systemu ERP w firmie).

Obecnie system CRAMM posiada kolejne wersje dla średnich i małych przedsiębiorstw, ale należy pamiętać o każdorazowym sprawdzeniu ich aktualizacji prawnej, szczególnie w odniesieniu do ryzyk i możliwości dochodzenia praw poszkodowanego na drodze penalnej.

Schemat oddziaływań w systemach teleinformacyjnych (STI) na informację i jej atrybuty przedstawia rys. 6.

4. Systemy informacyjne i informatyczne

Ochrona informacji w przypadku systemu informacyjnego opartego w całości na technice informatycznej to przedsięwzięcia systemowe (programowo-sprzętowe).

Do działań zabezpieczających zaliczyć tutaj należy[12]:

- stosowanie określonych bezpiecznych procedur przy projektowaniu i produkcji sprzętu teleinformatycznego,
- stosowanie określonych bezpiecznych procedur przy projektowaniu, kodowaniu, produkcji i dystrybucji oprogramowania,
- stosowanie odpowiednich programów operacyjnych (wewnętrzne narzędzia bezpieczeństwa programu, wprowadzanie praw dostępu, zabezpieczanie zbiorów i stanowisk pracy odpowiednimi hasłami lub narzędziami systemowymi),
- wykonywanie bezpiecznych instalacji sprzętowych („gorąca rezerwa”, bezpieczeństwo zasilania, równoległość pracy, dodatkowe macierze itp.),
- stosowanie urządzeń i procedur do odtwarzania STI (*backup*, DRP itp.),
- kodowanie i szyfrowanie informacji jak i nośników z jej zbiorami.

Szczególnym elementem jest tutaj przewidywanie potencjalnych zagrożeń dla bezpieczeństwa systemu informacyjnego realizowanego przy wykorzystaniu projektowanego STI, co schematycznie przedstawia rys. 7[13]:

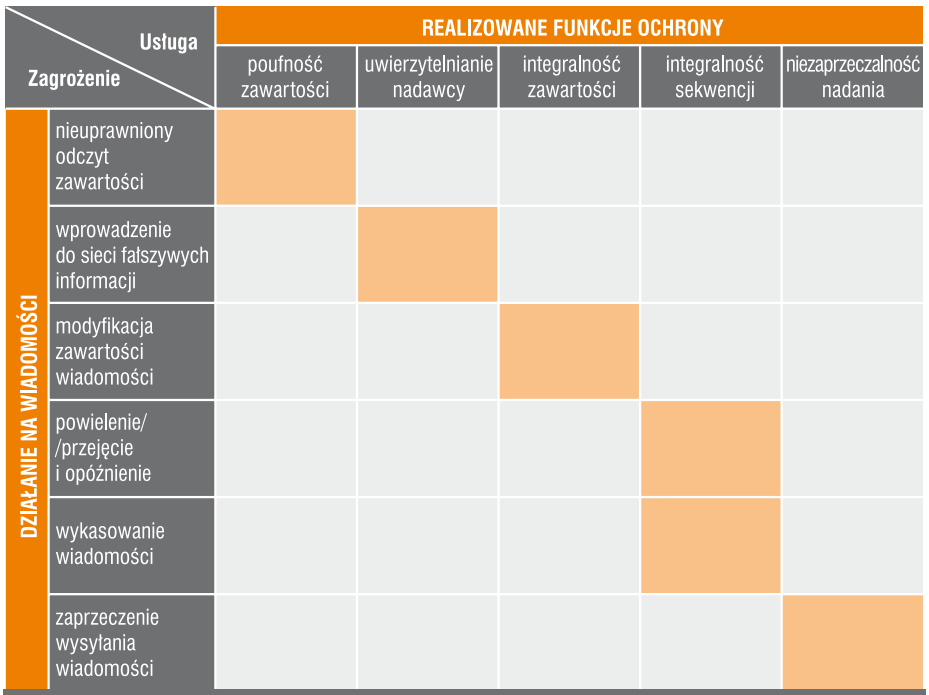
Za główne należy jednak uznać działanie na korzyść ochrony wewnętrznych i zewnętrznych połączeń komunikacyjnych STI. Systemy teleinformatyczne charakteryzują się bowiem pod względem swego wykorzystania w procesach informacyjnych dwoma elementarnymi procesami:

- przetwarzaniem informacji w samym systemie,
- przesyłaniem informacji między systemami,

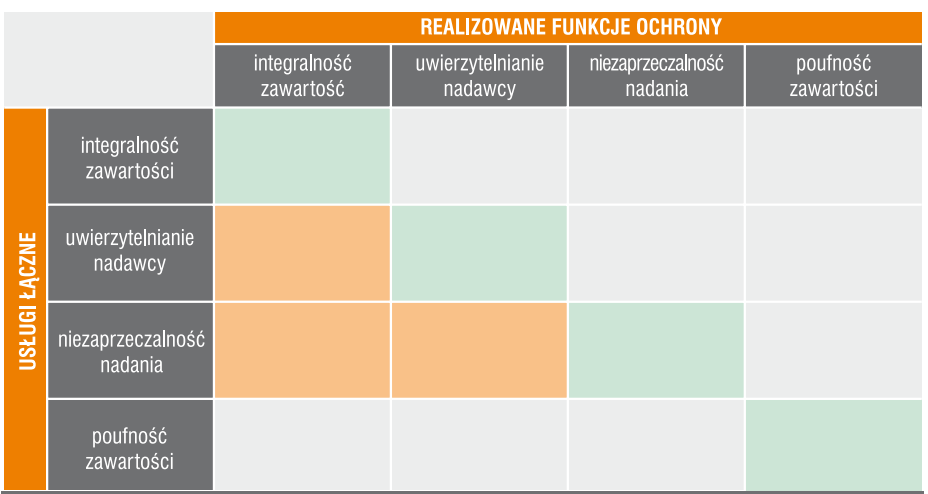
co wiąże się z odpowiednimi funkcjami obsługi i usługami

12) A. Białas: *Podstawy bezpieczeństwa systemów teleinformatycznych,* wyd. J. Skalmierskiego, Gliwice, 2002.

13) M. Blim: *Zarządzanie jakością i bezpieczeństwem systemów TI,* materiały szkoleniowe IOP PW, Warszawa, 2004.



Rys. 8. Realizowane w STI funkcje ochrony informacji przesyłanych



Rys. 9. Realizowane w STI usługi łączne ochrony informacji przesyłanych

systemowymi, a zarazem wymaga odpowiednich uprawnień w zakresie dostępu i czynności wobec zbiorów/zasobów informacyjnych, bo nawet wiadomości przekazywane w obrębie firmy są narażone na rozmaite niepożądane oddziaływania, stąd konieczne są funkcje ochrony dla systemu ich przemieszczania (od adresata do odbiorcy – z niezbędną wiarygodnością działań)[14].

Należy przy tym pamiętać, że w przypadku systemów teleinformatycznych można stosunkowo łatwo spełniać łącznie wymogi poszczególnych kryteriów, ale istotna staje się wówczas dostępność nie tyle informacji, ile aktywów całego systemu.

Brak dostępu do istotnych informacji może zagrozić katastrofą, w rozumieniu niemożliwości realizacji planowanych lub oczekiwanych działań biznesowych. Z tego też tytułu dostępność aktywów technologii informatycznej jest na ogół klasyfikowana do jednej z wymienionych poniżej czterech klas bezpieczeństwa: T1 – T4[15].

Działaniem pochodnym jest przyjęcie jednakowych narzędzi zapewniających: uwierzytelnienie nadawcy, integralność przesyłki, niezaprzeczalność nadania i odbioru, poufność przesyłki, bezpieczeństwo transmisji oraz dostępność systemu i informacji w nim (tab. 1).

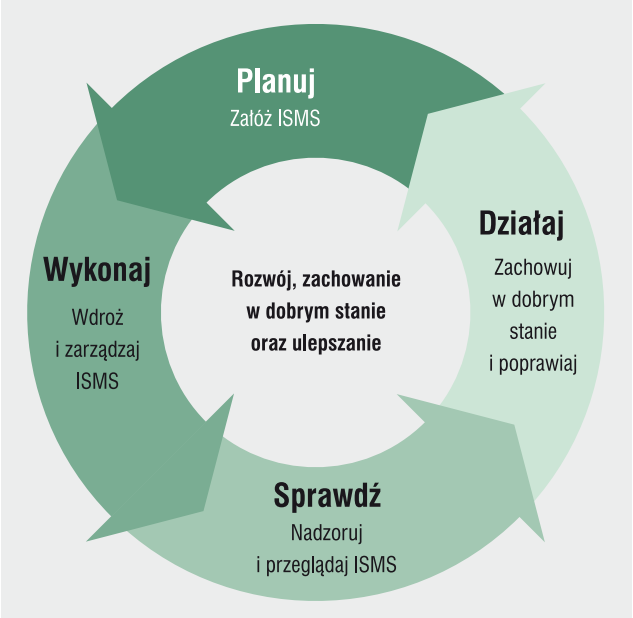
Należy mieć świadomość tego, że przytoczone powyżej opisy działań systemowo- technicznych są przykładowe, a nad ciągłością działania i prawidłowym przebiegiem procesów komunikacyjnych czuwają osoby funkcyjne o odpowiednich uprawnieniach i wyposażone w niezbędne narzędzia systemowe.

5. Wybór dobrej idei

W wyniku przeprowadzonych kolejnych etapów analizy funkcjonalnej (zob. AF – cz. I) problemu ochrony informacji stajemy wobec idealistycznego kryterium, jakim jest wybór rozwiązania ze względu na ustalone cele końcowe. W odniesieniu do reguł biznesowych (*cięcie kosztów – maksymalizacja zysków*) nagminne są sytuacje, kiedy to menedżer, mówiąc o ochronie informacji, wcale nie

Klasa dostępności	Kryteria	Postanowienia
Niekrytyczna (T1)	Informacja lub funkcja systemu, bez której można się obejść przez długi czas. **Dopuszczalna jest niedostępność przez miesiąc.**	Brak określonej granicy katastrofy
Mniej krytyczna (T2)	Informacja lub funkcja systemu, bez której można się obejść przez krótki okres z mniejszymi konsekwencjami. **Niedostępność przez tydzień jest do przyjęcia.**	Granica katastrofy wynosi **trzy tygodnie**
Krytyczna (T3)	Informacja lub funkcja systemu, która jest niezbędna dla realizacji celów operacyjnych. Poważne konsekwencje w przypadku niedostępności informacji lub funkcji. **Informacja lub funkcja systemu musi być ponownie dostępna w ciągu 24 godzin.**	Granica katastrofy wynosi **72 godziny**
Wysoko krytyczna (T4)	Informacja lub funkcja systemu, która jest niezbędna dla znaczącej części całości działalności. Bardzo poważne konsekwencje w przypadku niedostępności informacji lub funkcji (tzn. brak możliwości prowadzenia działalności). **Informacja lub funkcja systemu musi być ponownie dostępna w ciągu kilku godzin.**	Granica katastrofy wynosi 24 **godziny**

Tab. 1. Realizowane w STI usługi łączne ochrony informacji przesyłanych



Rys. 10. Model PDCA

chce jej ulepszać czy poprawiać – chce zaoszczędzić na wydatkach na ochronę i bezpieczeństwo informacji.

Panowie prezesi i menedżerowie głównych procesów w licznych instytucjach po prostu zapominają, że bezpieczeństwo informacji nie jest stanem – ono jest procesem o fluktuacjach bardzo trudnych chwilami do przewidzenia. Wszystko jest zależne od przyjętych w danej firmie kryteriów oceny wartości dla systemu informacyjnego i objętych jego działaniami zasobów.

6. Chwila refleksji...

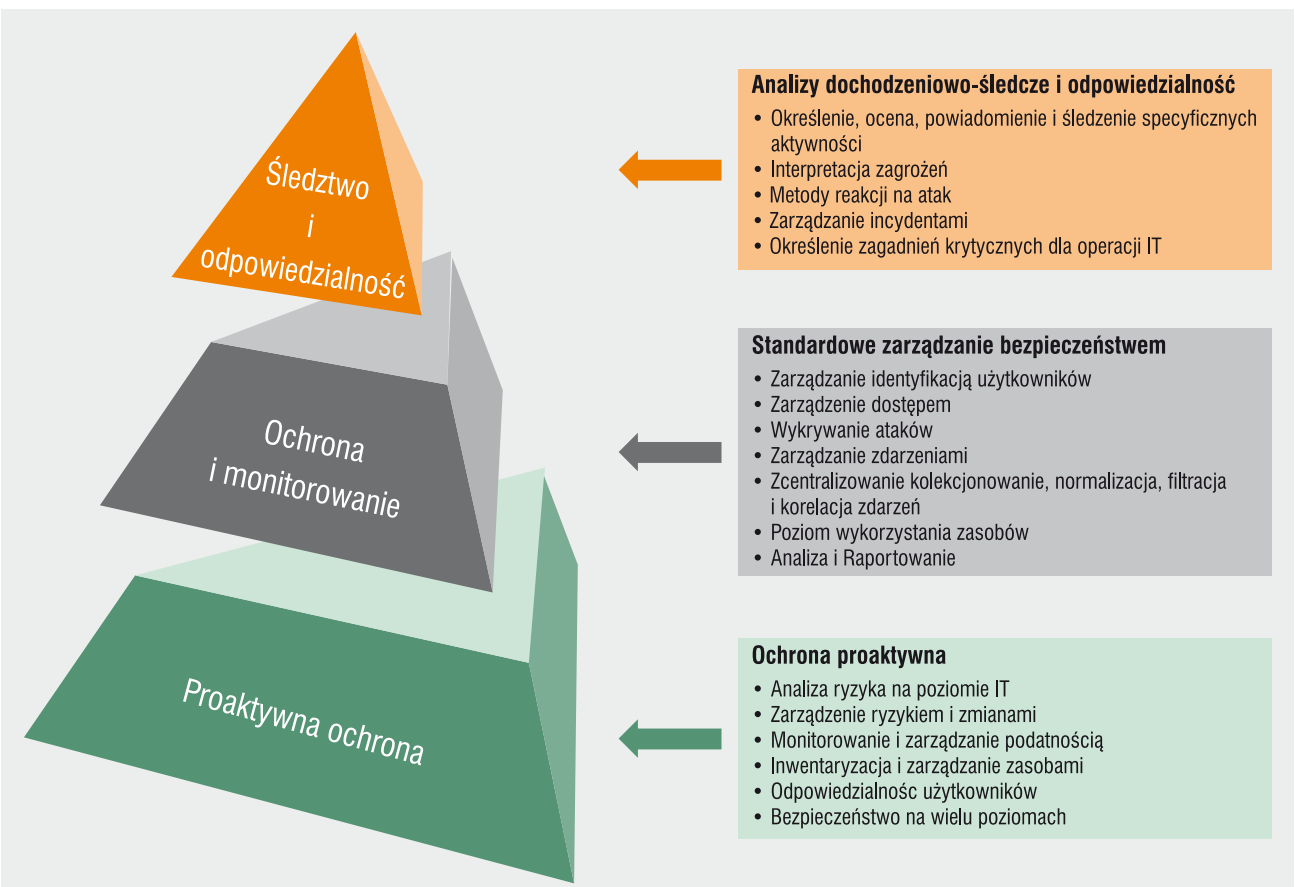
Normy bezpieczeństwa opierają się na zasadach ogólnych zarządzania jakością (ISO 9001) oraz na cyklu Deminga (PDCA – *Plan–Do–Check–Act*), co widać również w odniesieniu do ISMS na rys. 10.

Ale decydujące dla całości teoretycznych i praktycznych działań w ochronie informacji jest przestrzeganie kilku podstawowych założeń:

1. Ochrona STI musi być prowadzona jako proaktywna, istotne jest użytkowanie systemu, a nie jego naprawianie i ściganie winnych – choć i tego nie wolno zaniedbać.
2. Tylko świadomość wszystkich zaangażowanych osób (zarządzających, użytkowników, eksploatatorów, projektantów oraz pionów ochrony bezpieczeństwa informacji na każdym z etapów) pozwoli na wykrycie i wyeliminowanie krytycznych incydentów, zanim staną się one kłopotliwymi zdarzeniami (oby nie katastrofami).
3. Trzeba planować koszty zachowania oraz ciągłość inwestowania w realizowanych/przyszłych procesach ochrony i bezpieczeństwa informacji.

O czym, po raz kolejny, pozwalam sobie przypomnieć wszystkim zainteresowanym...

OPRACOWAŁ:
DR INŻ. MAREK BLIM



Rys. 11. Model proaktywnej ochrony informacji

14) M.Blim: *Zarządzanie bezpieczeństwem obiektu,* skrypt kursu instalatorów SA-4, wyd. Techom, Warszawa, 2004.
15) tamże.

Bibliografia:

1. Normy:
   - PN-ISO/IEC 17799:2007 Bezpieczeństwo informacji. Systemy zarządzania bezpieczeństwem informacji. Praktyczne zasady zarządzania bezpieczeństwem informacji
   - PN-ISO/IEC 27001:2007 Bezpieczeństwo informacji. Systemy zarządzania bezpieczeństwem informacji. Specyfikacja i wytyczne do stosowania
2. Anderson R.: *Inżynieria zabezpieczeń,* seria TAO, WNT, Warszawa, 2005.
3. Anonim (Sams): *Internet – agresja i ochrona,* Robomatic, Warszawa, 2003.
4. Beynon-Davies P.: *Inżynieria systemów informacyjnych,* WNT, Warszawa, 2002.
5. Białas A.: *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,* WNT, Warszawa, 2006.
6. Białas A.: *Podstawy bezpieczeństwa systemów teleinformatycznych,* wyd. Jacka Skalmierskiego, Gliwice, 2002.
7. Blim M.: *Zarządzanie bezpieczeństwem obiektu,* skrypt kursu instalatorów SA-4, Techom, Warszawa, 2004.
8. Blim M.: *Zarządzanie jakością i bezpieczeństwem systemów TI,* materiały szkoleniowe IOP PW, Warszawa, 2004.
9. Byczkowski M., Blim M., J. Zawiła-Niedźwiecki: *Zarządzanie ryzykiem operacyjnym w świetle wymogów Komitetu Bazylejskiego,* T. V, materiały konferencyjne XVI Szkoły Górskiej PTI, Szczyrk, 2004.
10. Dolińska I.: *Sieci komputerowe,* WSE-I, Warszawa, 2005.
11. Frankowski P.: *Komputerowi detektywi. 111 porad,* Mikom, Warszawa, 2003.
12. Gałach A.: *Instrukcja zarządzania bezpieczeństwem systemu informatycznego,* ODDK, Gdańsk, 2004.
13. Kaczor P.: *Hacking, cracking, phreacking, czyli ochrona przed cyberoszustami,* MIKOM, Warszawa, 2004.
14. Konieczny J.: *Wprowadzenie do bezpieczeństwa biznesu,* Konsalnet SA, Warszawa.
15. Krupa T.: *Wybrane aspekty zarządzania wiedzą w przedsiębiorstwach UE,* Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, Opole, 2006.
16. Lam K., LeBlanc, Smith B.: *Ocena bezpieczeństwa sieciowego,* APN Promise, Warszawa, 2005.
17. Liderman K.: *Standardy w ocenie bezpieczeństwa teleinformatycznego,* Biuletyn IAiR Nr 17, WAT, Warszawa, 2000.
18. Liderman K.: *Bezpieczeństwo teleinformatyczne,* wydanie 1, IAiR WAT, Warszawa, 2001.
19. Lukatsky A.: *Wykrywanie włamań i aktywna ochrona danych. Elita rosyjskich hakerów prezentuje Ну Погоди!*, Helion, Gliwice, 2003.
20. Mandia K., Proise C.: *Hakerom śmierć!,* RM, Warszawa, 2002.
21. McNamara: *Arkana szpiegostwa komputerowego,* Helion, Gliwice, 2001.
22. Pipkin D. L.: *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa,* seria TAO, WNT, Warszawa, 2002.
23. *Bezpieczeństwo od A do Z,* wydanie 17, Wiedza i Praktyka, Warszawa, styczeń 2004.
24. *Informatyka. Terminologia znormalizowana i wykaz norm,* praca zbiorowa, PKN, Warszawa, 2006.

ESSER
by Honeywell

Honeywell

high-end **solutions**

SAP SWN KD DSO

najlepsze **rozwiązania**

Alpol Sp. z o.o. dystrybutor Honeywell Life Safety (SSP ESSER, Systemy Przywoławcze ACKERMANN i DSO ESSER-SINAPS) oraz Honeywell Security.

ALPOL HURTOWNIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

tel: 0 801 77 77 90

Bielsko-Biała	Gliwice	Katowice	Kraków	Lublin	Łódź
0 32 7907621	0 32 7907623	0 32 7907656	0 32 7907646	0 32 7907650	0 32 7907625
Poznań	Sopot	Szczecin	Warszawa Mokotów	Warszawa Praga	Wrocław
0 32 7907637	0 32 7907643	0 32 7907630	0 32 7907634	0 32 7907633	0 32 7907627

alpol@e-alpol.com.pl www.e-alpol.eu www.e-alpol.com.pl

MECHANIZMY ZABEZPIECZEŃ
w sieciach WiMAX

W artykule przedstawiono mechanizmy zapewniające bezpieczeństwo w sieciach WiMAX. Omówiono zmiany dotyczące mechanizmów zabezpieczeń w kolejnych standardach rodziny 802.16, które miały na celu poprawienie wykrytych podatności. Przeanalizowano również potencjalne luki, które mogą być wykorzystane w celu zaatakowania sieci WiMAX. W pierwszej części omówiono architekturę sieci WiMAX oraz najważniejsze pojęcia używane w dalszej części (takie jak asocjacja bezpieczeństwa, połączenie zarządzalne). Szczególny nacisk położono również na zaprezentowanie różnego typu połączeń występujących pomiędzy stacją bazową a terminalem abonenckim. Następnie opisano wszystkie etapy niezbędne do realizacji bezpiecznej wymiany danych dla stacji abonenckiej działającej w sieci WiMAX. Szczegółowo scharakteryzowano przebieg procesu uwierzytelniania z wykorzystaniem certyfikatów cyfrowych, sposób generowania i wymiany kluczy oraz ich późniejsze wykorzystanie do zapewnienia usług ochrony informacji. Przedstawiono również opis specjalistycznej infrastruktury klucza publicznego (PKI), którą będą musieli stworzyć producenci sprzętu i operatorzy sieci WiMAX.

Wprowadzenie do sieci WiMAX

Celem niniejszego rozdziału jest krótka charakterystyka sieci WiMAX (*World Interoperability for Microwave Access*) – IEEE 802.16 [4, 5], porównanie ich z sieciami WiFi (IEEE 802.11) [1, 2] oraz wskazanie możliwych kierunków rozwoju sieci opartych na standardzie 802.16.

Popularność sieci WiFi pokazała, jak wygodnym rozwiązaniem jest bezprzewodowy dostęp do sieci teleinformatycznych. Najlepiej o popularności tego typu sieci świadczą wbudowane fabrycznie w laptopy karty WiFi i pojawiające się w wielu miejscach darmowe punkty dostępowe (HotSpoty). Największym problemem w pierwszym okresie wdrażania sieci WiFi stała się ochrona transmisji danych, która spowodowała, że długo sieci te nie były uważane za bezpieczne. Dopiero wprowadzenie standardu 802.11i [3] pozwala na budowanie sieci WLAN gwarantujących bezpieczeństwo przesyłanych danych. Drugim, do tej pory nierozwiązanym zagadnieniem, jest stosunkowo mały zasięg sieci WiFi. Jednak zmiany w tym aspekcie najpewniej nie zostaną wprowadzone, a panaceum jest wykorzystanie innych standardów sieciowych, np. WiMAX. W sieciach WiMAX będzie możliwe uzyskanie zasięgu dochodzącego nawet do kilkunastu kilometrów. Pierwszym i jak na razie głównym zastosowaniem tych sieci jest tzw. ostatnia mila, czyli odcinek pomiędzy siedzibą abonenta a najbliższym urządzeniem komutującym należącym do operatora. Dlatego też sieci WiMAX znajdują zastosowanie przede wszystkim w terenie słabo zurbanizowanym, tym bardziej że możliwa jest praca sieci w trybie NLOS *(Non Line Of Sight)*, czyli kiedy odbiornik nie musi „widzieć" anteny. Podstawową zaletą tego trybu jest prostota instalacji, bez skomplikowanego podłączania anteny urządzenia abonenckiego w sposób wymagający widoczności stacji bazowej. Jednak sieci WiMAX oferują nie tylko tryb stacjonarny (dokładniej nomadyczny), w nowszych wersjach zapewniona jest pełna mobilność użytkowników, przez wprowadzenie znanego z sieci komórkowych mechanizmu *handover*. Mechanizm ten umożliwia przezroczyste przenoszenie całego stanu sesji komunikacyjnej do innej stacji bazowej, gwarantującej lepszą jakość sygnału. Wprowadzanie tego mechanizmu wraz z zapewnieniem większej przepustowości, w porównaniu z sieciami komórkowymi, może spowodować uruchomienie za pomocą tej technologii dostępu do usług takich jak cyfrowe radio i telewizja czy usług typu wideo na żądanie (*Video on Demand*, VoD).

Co ważne i godne podkreślenia, aspekty związane z bezpieczeństwem były rozpatrywane i zostały uwzględnione już na początku prac nad standardem sieci WiMAX. Nie grozi zatem sytuacja z początków wdrażania standardu 802.11, gdy okazało się, że nie jest możliwe zbudowanie sieci gwarantujących wysokie bezpieczeństwo ich użytkownikom. Z tego powodu w stosie protokołów WiMAX została wprowadzona specjalna podwarstwa odpowiedzialna za zapewnienie bezpieczeństwa komunikującym się urządzeniom (*Security Sublayer*). W tej podwarstwie realizowane jest uwierzytelnianie komunikujących się stron oraz zapewnianie poufności i integralności przesyłanych danych. Więcej informacji na ten temat znajduje się w dalszej części artykułu.

Zagrożenia związane z sieciami radiowymi

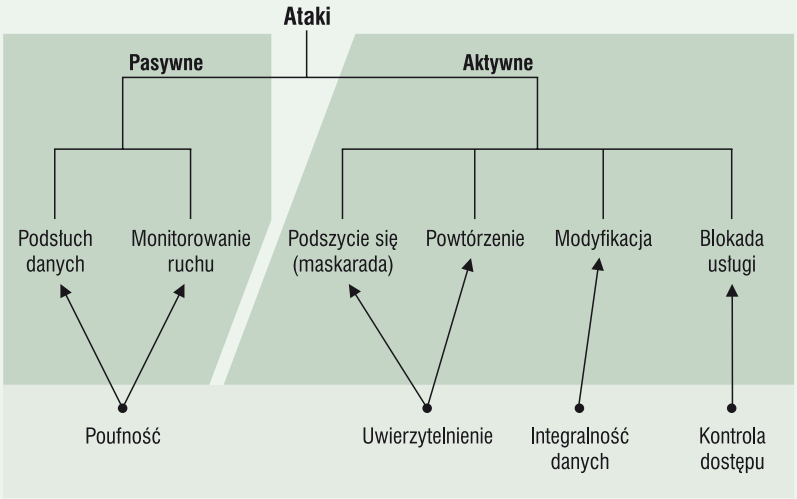
Zagrożenia, na jakie narażona jest sieć WiMAX, są typowe dla sieci radiowych. Rozważana przez nas taksonomia ataków wyróżnia następujące ataki:

a) pasywne – nieautoryzowana działalność, w której atakujący nie modyfikuje zawartości ramek, a jedynie biernie nasłuchuje transmisji w kanale:
   - podsłuch danych – atakujący przechwytuje informacje wymieniane pomiędzy legalnymi użytkownikami,
   - monitorowanie ruchu – intruz śledzi transmisje pomiędzy legalnymi użytkownikami w celu analizy cech stacji i ich aktywności,

b) aktywne – nieautoryzowana działalność, w której atakujący czynnie bierze udział w transmisji w kanale:
   - podszycie się (maskarada) – atakujący udaje legalnego użytkownika lub usługę sieciową,
   - powtórzenie – włamywacz po przechwyceniu za pomocą podsłuchu informacji retransmituje ją tak jak legalny użytkownik,
   - modyfikacja – intruz kasuje, dodaje, zmienia wiadomość wysłaną przez legalnego użytkownika,

– blokada usługi – atakujący destabilizuje pracę sieci, uniemożliwiając poprawną komunikację.

Na rys. 1 taksonomia została przedstawiona w sposób graficzny. Pod rodzajami ataków zostały wymienione usługi ochrony informacji, które mogą zminimalizować lub przy prawidłowym wdrożeniu zredukować praktycznie do zera część z wymienionych zagrożeń.



Rys. 1. Podział ataków na sieć WiMAX

Jak wspomniano, tworząc standard WiMAX, starano się uniknąć błędów popełnionych przy opracowywaniu standardu 802.11. Wykorzystano silne algorytmy kryptograficzne, aby zapewnić usługi ochrony informacji. W celu zapewnienia poufności danych, zastosowano algorytmy symetryczne DES (*Data Encryption Standard*), 3DES (*Triple DES*), AES (*Advanced Encryption Standard*) oraz asymetryczny RSA (Rivest, Shamir, Adleman). Z wyjątkiem algorytmu DES, który z powodu długości klucza dzisiaj jest już nie zalecany, chociaż nadal jest o wiele silniejszy niż stosowany powszechnie w sieciach WiFi mechanizm WEP (*Wired Equivalent Privacy*), pozostałe algorytmy uważane są za bezpieczne. Aby zapewnić integralność danych, zostały użyte natomiast mechanizmy rodziny MAC: HMAC (*Keyed-Hash Message Authentication Code*) lub CMAC (*Cipher-based Message Authentication Code*). Za zapewnienie autoryzacji oraz uwierzytelnienia odpowiedzialny jest protokół PKM (*Privacy Key Management*). Wykorzystuje on m.in. szyfrowanie asymetryczne i certyfikaty klucza publicznego wystawiane dla każdego urządzenia działającego w sieci WiMAX.

Oprócz wymienionych powyżej podstawowych usług ochrony informacji nie można zapomnieć o zarządzaniu kluczami. Brak tych mechanizmów w sieciach WiFi spowodował, że w początkowym okresie ich rozwoju szyfrowanie danych było często wyłączane z powodu braku protokołów dystrybucji kluczy. W WiMAX wymiana kluczy jest nierozerwalnie związana z procesem logowania do sieci i uwierzytelnianiem stacji. Usługa zarządzania kluczami w sieciach WiMAX wspierana jest również przez wspomniany wyżej protokół PKM.

Architektura bezpieczeństwa sieci WiMAX

Sieci WiMAX mogą działać w dwóch trybach – trybie punkt-wielopunkt oraz trybie kraty. Pierwszy z wymienionych w dzisiejszych zastosowaniach wydaje się najpraktyczniejszy. Punktem centralnym jest stacja bazowa, za pomocą której komunikują się wszystkie pozostałe urządzenia w sieci WiMAX. Jest to także miejsce styku z innymi sieciami podłączonymi kablem. Mamy tutaj sytuację podobną do sieci WiFi działającej z punktem dostępowym (*Access Point*, AP). Tryb kraty wydaje się interesującym rozwiązaniem w sytuacji, kiedy pewne stacje bazowe nie mają bezpośredniej łączności z częścią przewodową sieci. W takim wypadku zamiast łącza przewodowego do sieci zewnętrznej wykorzystywane jest połączenie radiowe do innej stacji bazowej. Tryb kraty, gdzie każde urządzenie abonenckie mogłoby komunikować się z każdym, wydaje się niepraktyczny, tym bardziej że urządzenia abonenckie mają ograniczoną moc nadajnika. Z tego powodu tryb kraty nie będzie w dalszej części artykułu omawiany.

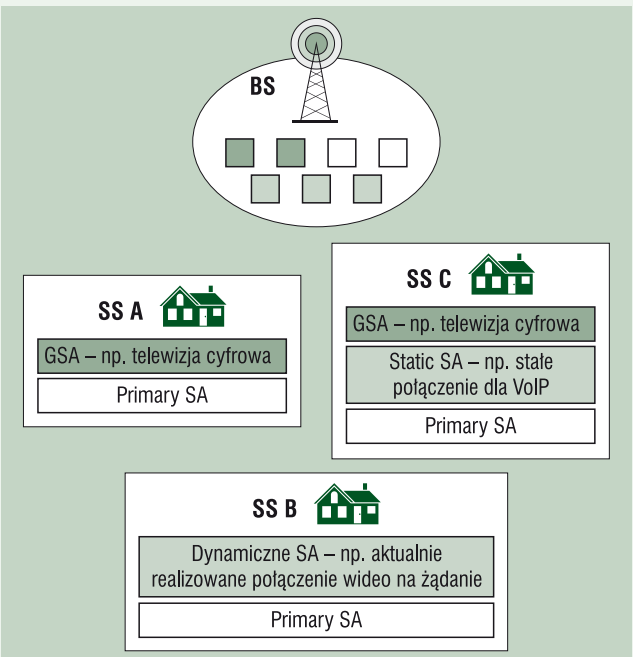
Wszystkie urządzenia abonenckie (*Subscriber Station*, SS) komunikują się ze stacją bazową (*Base Station*, BS). Stacja bazowa odpowiedzialna jest za zarządzanie pasmem i zezwala na transmisję poszczególnych urządzeń. Każde urządzenie w sieci WiMAX posiada adres MAC, za pomocą którego jest identyfikowane. Przy aktualnych standardach możliwe jest przesyłanie za pomocą sieci WiMAX danych, wykorzystując protokoły ATM, 802.3 (ramki ethernetowe), 802.1q (ramki ethernetowe różnych VLAN-ów) oraz pakiety IPv4 i IPv6. Co ciekawsze, możliwe jest stworzenie wielu niezależnych strumieni danych dla każdego urządzenia działającego w sieci. Każde takie połączenie posiada wynegocjowane oddzielnie parametry bezpieczeństwa. Wszystkie informacje na temat parametrów bezpieczeństwa przechowywane są w strukturze danych, zwanej asocjacją bezpieczeństwa (*Security Association*, SA). W niej przechowywane są dane pozwalające na zaszyfrowanie, odszyfrowanie czy sprawdzenie integralności przesyłanych danych. Tutaj znajdują się informacje o wynegocjowanych i aktualnie używanych algorytmach kryptograficznych, aktualnie używane klucze, ich czasy obowiązywania oraz wszelkie inne informacje potrzebne do normalnej pracy algorytmów kryptograficznych. Dla ustalonego zestawu algorytmów utrzymywane są dwa komplety informacji odpowiadające możliwym do wykorzystania kluczom – starszemu i nowszemu. Takie podejście pozwala na przechodzenie z jednego klucza, którego czas obowiązywania się zakończył, do następnego. Nie zdarza się, że klucz z powodu cyklicznej zmiany jest nieaktualny. Dla każdego połączenia muszą istnieć odpowiadające sobie asocjacje bezpieczeństwa w SS i BS rozróżniane przez identyfikator SAID *(Security Association ID*).

Mając na uwadze przyszłe zastosowania sieci WiMAX, wprowadzono kilka rodzajów połączeń i odpowiadających im asocjacji bezpieczeństwa. Każda SS posiada co najmniej jedną podstawową asocjację bezpieczeństwa (*Primary SA*) odpowiedzialną za obsługę połączenia służącego do zarządzania komunikacją pomiędzy parą SS i BS. Te połączenie jest wykorzystywane jedynie przez te dwa urządzenia. Poza nim możliwe jest utworzenie dowolnej liczby tzw. statycznych asocjacji pomiędzy daną SS i BS. Za ich pomocą mogą być przesyłane inne dane, przykładowo ruch telefonii VoIP (*Voice over IP*) czy zwykłe dane komputerowe.

Oprócz opisanych powyżej statycznych asocjacji w standardzie 802.16 zostały wprowadzone jeszcze dwa rodzaje asocjacji – dynamiczne i grupowe. Asocjacje dynamiczne tworzone są na specjalne życzenie stacji klienckiej za pomocą komunikatów DSA-XXX. Wysłanie tych komunikatów, czyli podjęcie decyzji o nawiązaniu nowego połączenia, jest sterowane przez oprogramowanie warstw wyższych. Przykładowo, nowe połączenie może być nawiązane w celu uzyskania zamówionego materiału (wideo na żądanie) czy skonfigurowania nowego kanału wirtualnego (*Virtual Channel*, VC) lub ścieżki (*Virtual Path*, VP) w przypadku, gdy stacja abonencka działa jak urządzenie ATM (*Asynchronous Transfer Mode*).

Asocjacje grupowe (*Group Security Association*, GSA) służą do obsługi ruchu typu multicast (transmisja do wielu odbiorców, stanowiących jedną grupę) lub broadcast (rozgłoszeniowy tryb transmisji) w sieciach WiMAX. Połączenia te mogą być efektywnie wykorzystane do transmisji cyfrowej telewizji czy cyfrowego radia za pomocą sieci WiMAX. Jak sugeruje sama nazwa, transmisja tego typu jest odbierana przez wiele stacji. Żeby ułatwić proces zmiany kluczy w tym trybie transmisji, nowe klucze są przesyłane w komunikatach *Group Key Update* do wszystkich zainteresowanych stacji.

Na rys. 2. przedstawiony jest stan przykładowej sieci WiMAX składającej się z jednej BS i trzech stacji SS.

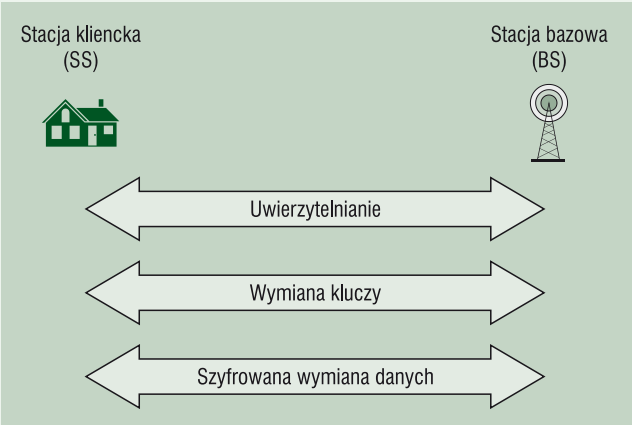


Rys. 2. Przykłady komunikacji w sieci WiMAX oraz odpowiadające im asocjacje bezpieczeństwa

Schematycznie za pomocą różnokolorowych kwadratów zaznaczone są asocjacje bezpieczeństwa wynegocjowane podczas procesu logowanie do sieci WiMAX. Wszystkie stacje posiadają po jednej głównej asocjacji bezpieczeństwa. Poza nią mają jeszcze inne połączenia służące do wymiany pozostałych danych. Przykładowo, stacja B posiada dynamicznie wynegocjowane połączenie, przez które dostarczany jest do klienta zamówiony film. Stacja C posiada statyczną asocjację odpowiedzialną za obsługę połączeń VoIP. Jak wspomniano, w niektórych przypadkach przydatna jest możliwość wykorzystania transmisji z jednego urządzenia do wielu. Przykładem idealnego zastosowania takiego rozwiązania jest np. transmisja telewizji cyfrowej. Ponieważ dane tego typu są identyczne dla wielu odbiorców, opłacalna wydaje się transmisja jednego strumienia danych odbieranego przez wielu odbiorców. Na rys. 2. w ten sposób dostarczana jest telewizja cyfrowa dla stacji A i C. Co warte podkreślenia, każde z przedstawionych połączeń ma oddzielnie wynegocjowane parametry bezpieczeństwa. Nie jest możliwe zatem, aby jakiekolwiek dane zostały odczytane przez nieuprawnione osoby.

Logowanie urządzenia w sieci

Ogólny przebieg procesu podłączenia się i uzyskiwania dostępu w sieciach WiMAX przedstawiono na rys. 3.



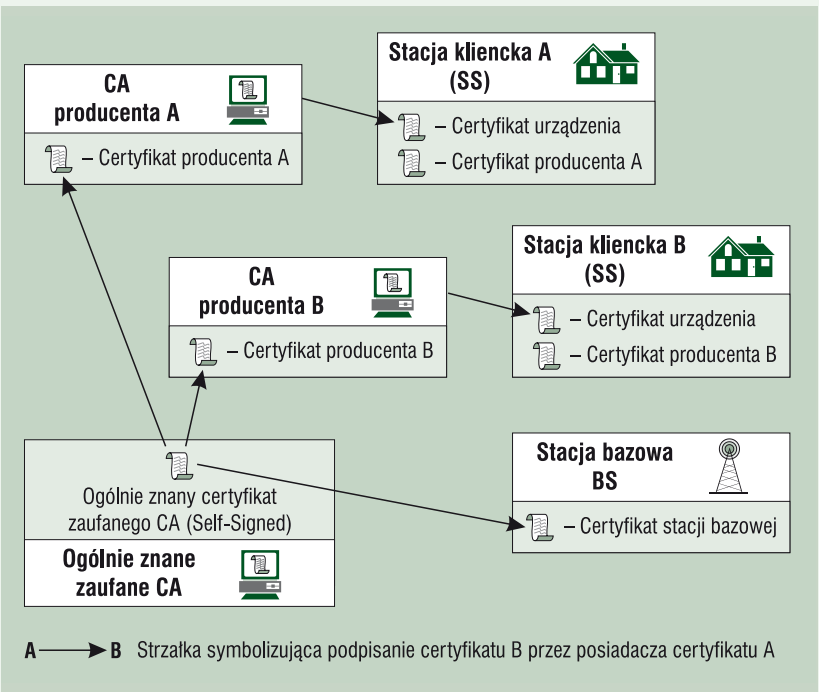
Rys. 3. Ogólny schemat wymiany informacji pomiędzy stacją kliencką a stacją bazową

Proces uwierzytelniania

Każde urządzenie abonenckie musi przejść proces uwierzytelniania w stacji bazowej, aby móc wymieniać informacje z innymi urządzeniami w sieci WiMAX lub uzyskać dostęp do innych urządzeń podłączonych do stacji bazowej łączem kablowym. Uwierzytelnianie realizowane jest za pomocą certyfikatów cyfrowych standardu X.509. Każde urządzenie abonenckie w sieci WiMAX zgodnie ze standardem powinno posiadać dwa certyfikaty. Pierwszy jest certyfikatem producenta; w skład jego opisu powinny wchodzić: nazwa kraju oraz nazwa producenta. Certyfikat ten umożliwia sprawdzenie autentyczności certyfikatu urządzenia. Może on być podpisany przez samego producenta (*Self-signed Certificate*). Podpisanie go przez ogólnie znaną organizację, zajmującą się poświadczaniem certyfikatów, zwiększa bezpieczeństwo. W takim przypadku operator może niezależnie sprawdzić autentyczność certyfikatu producenta, wysyłanego do stacji bazowej podczas wstępnej fazy uwierzytelniania urządzenia w sieci. Drugim certyfikatem jest indywidualny certyfikat stacji abonenckiej. W jego skład powinna wchodzić: nazwa producenta urządzenia, kraj produkcji oraz numer seryjny i adres MAC stacji abonenckiej. Najbezpieczniejszym rozwiązaniem wydaje się generowanie obu certyfikatów w procesie produkcji urządzenia. Jednak standard przewiduje możliwość wygenerowania kluczy i certyfikatów samoczynnie przez urządzenie. W tej sytuacji klucze i certyfikat muszą być wygenerowane przed próbą włączenia się danego urządzenia do sieci.

Na rys. 4. zaprezentowano schemat pokazujący, jakie certyfikaty biorą udział w procesie uwierzytelniania stacji SS.

Wszystkie etapy uwierzytelniania realizowane są przez protokół PKM (*Privacy Key Management*). W standardzie 802.16e-2005 [3] została zdefiniowana nowa wersja protokołu PKMv2. Przewidziano w niej możliwość uwierzytelniania stacji bazowych, co wiąże się z wygenerowaniem certyfikatów dla każdej stacji. Certyfikaty stacji bazowej powinny zawierać nazwę kraju, nazwę operatora oraz numer seryjny i unikatowy w sieci operatora identyfikator stacji. Zmiana ta przy prawidłowym wdrożeniu bezpieczeństwa uniemożliwi podszycie się atakującego pod stację bazową i przeprowadzenie ataków przechwytywania przez podmiot pośredniczący (*Man In The Middle*). Oprócz tego wprowadzono możliwość skorzystania z serwera AAA (*Authentication Authorization Accounting*) za pomocą protokołów rodziny EAP (*Extensible Authentication Protocol*) [9].



Rys. 4. Infrastruktura Klucza Publicznego (PKI) w sieciach WiMAX

Szczegółowy opis protokołów PKMv1 i PKMv2 zawarty został w [7].

Proces wymiany kluczy

Po pomyślnym uwierzytelnieniu następuje faza odpowiedzialna za uzgodnienie używanych algorytmów kryptograficznych i wymianę kluczy, także realizowana przez protokół PKM. Jej bezpieczeństwo opiera się na algorytmie RSA i kluczach publicznych zawartych we wcześniej wymienianych certyfikatach. Ze względów wydajnościowych w obu protokołach PKM są stworzone hierarchie kluczy i jedynie klucz główny jest wymieniany w ten sposób. Efektem tej fazy jest uzgodnienie pomiędzy stacją bazową a kliencką klucza AK (*Authorization Key*). Klucz ten (lub pre-AK w PKMv2), jak wspomniano, podczas transportu do stacji abonenckiej zaszyfrowany jest za pomocą publicznego klucza algorytmu RSA. Wykorzystywany jest tutaj algorytm RSA zgodny ze specyfikacją PKCS #1 (*Public-Key Cryptography Standards*). Klucz jest 1024-bitowy, a publicznie znany wykładnik przyjmuje wartość 65 537 (0x010001). Klucz publiczny przekazywany jest do stacji bazowej w certyfikacie zgodnym z protokołem X.509.

Na podstawie wcześniej uzgodnionego klucza generowane są klucze KEK (*Key Encryption Key*), które służą do zabezpieczenia kluczy sesyjnych TEK (*Traffic Encryption Key*). Te ostatnie służą do bezpiecznej wymiany danych użytkowych. Aktualnie w sieciach WiMAX do szyfrowania kluczy TEK można wykorzystać jeden z czterech następujących algorytmów: 3DES w trybie EDE (*Encryption Decryption Encryption*) ze 128-bitowym kluczem, RSA z 1024-bitowym kluczem, AES w trybie ECB (*Electronic Code Book*) z 128-bitowym kluczem i dodany w standardzie 802.16e-2005 AES w trybie Key-Wrap ze 128-bitowym kluczem.

Proces szyfrowanej wymiany danych oraz zapewnienia integralności

Po zakończeniu fazy wymiany kluczy stacja abonencka powinna mieć stworzone lokalnie wszystkie statyczne asocjacje bezpieczeństwa. Od tego momentu możliwa jest już w pełni bezpieczna wymiana danych zabezpieczonych we wcześniej wynegocjowany sposób (wybrany algorytm szyfrowania). Uzgodnione klucze są ważne przez ustalony okres, po którym są zmieniane. W celu nieprzerwanej pracy stacja bazowa utrzymuje po dwa komplety kluczy. Wszystkie dane użytkowe transmitowane w sieci mogą podlegać szyfrowaniu za pomocą jednego z algorytmów: DES (w trybie CBC) lub AES (w trybach CCM, CBC lub CTC).

Zapewnienie integralności w sieci WiMAX może dotyczyć dwóch rodzajów transmisji – danych użytkownika sieci i informacji zarządzających. Dla pierwszego przypadku w momencie konfiguracji można zdecydować, że transmitowane ramki z danymi użytkowymi oprócz szyfrowania zostaną także uwierzytelnione. W tym celu używany jest algorytm AES w trybie CCM. W takim wypadku dane zostaną zaszyfrowane, a także do ramki zostanie dodany 8-bajtowy ICV (*Integrity Check Value*). Natomiast integralność wiadomości zarządzających jest zapewniana za pomocą algorytmów HMAC [10] w połączeniu z funkcją skrótu SHA-1 lub algorytmu CMAC [8]. W takim wypadku wybrane ramki zarządzania będą miały na końcu dodane pole, które zawiera kod uwierzytelniający wiadomość policzony dla aktualnej zawartości i zabezpieczony wcześniej uzgodnionym kluczem. Do wyliczania kodu uwierzytelniającego wiadomość używane są klucze ustalone w trakcie uwierzytelniania za pomocą protokołu PKM.

Potencjalne luki w zabezpieczeniach

Analiza stanu bezpieczeństwa sieci WiMAX wypada o wiele lepiej niż analiza stanu bezpieczeństwa sieci WiFi, nawet po kilku latach od ich upowszechnienia. Przy opracowywaniu standardu 802.16 nie popełniono błędów znanych z sieci WiFi. Główne różnice polegają na zastosowaniu odpowiednich algorytmów kryptograficznych (np. RSA, AES) oraz

wprowadzeniu wszystkich mechanizmów w początkowej wersji standardu (protokół PKM do zarządzania kluczami, PKI do zarządzania certyfikatami itp.). Jest jednak parę aspektów związanych z bezpieczeństwem, które mogą wpłynąć na obniżenie poziomu bezpieczeństwa sieci WiMAX. Największe wątpliwości budzą opcje umożliwiające wyłączenie z powodów wydajnościowych oraz z powodu potencjalnych problemów konfiguracyjnych wspieranych mechanizmów zabezpieczeń.

Dodatkowo w standardach 802.16 nie wspomniano o obowiązku skorzystania z certyfikatów producenta do sprawdzenia autentyczności przesyłanych certyfikatów urządzeń. Przesyłany certyfikat producenta urządzenia pełni jedynie rolę informacyjną. Nie wymuszono także tego, by był on podpisany przez wiarygodną organizację zajmującą się dostarczaniem certyfikatów, oraz aby sprawdzana była jego autentyczność. Braki te mogą prowadzić do pomniejszenia roli certyfikatów, co może wpłynąć na zmniejszenie poziomu bezpieczeństwa całej sieci. W praktyce może to sprawić, że takie rozwiązanie przestanie być przydatne.

Pamiętajmy, że producenci urządzeń muszą być godni zaufania, podobnie jak producenci kart SIM w telefonii GSM. To na nich spoczywa obowiązek odpowiedniego zabezpieczenia informacji związanych z procesem wgrywania i ewentualnego przechowywania informacji na temat kluczy prywatnych. Zatem to oni będą musieli stworzyć na potrzeby produkowanych urządzeń własne centra certyfikacji (*Certification Authority*, CA).

Jak wspomniano, wszystkie dane użytkowe transmitowane w sieci mogą być szyfrowane za pomocą algorytmu DES (w trybie CBC) lub AES (w trybach CCM, CBC lub CTC). Dla danych o mniejszym stopniu ważności lub urządzeń nieposiadających zaimplementowanych funkcji kryptograficznych można również wybrać brak szyfrowania. Najprostsze urządzenia bowiem nie byłyby w stanie wykonać skomplikowanych operacji kryptograficznych. Jednak z punktu widzenia bezpieczeństwa danych takie podejście może prowadzić do sytuacji z początków wdrażania sieci WiFi, kiedy użytkownicy wyłączali zabezpieczenia, nie chcąc utrudniać sobie pracy. Jedyną pociechą w tym wypadku jest, że standard przewidział możliwość odmówienia uwierzytelnienia stacji, która nie obsługuje wymaganych w danej sieci standardów bezpieczeństwa.

Niebezpieczna może być również rezygnacja z szyfrowania wiadomości zarządzających, poza tymi niosącymi klucze. Brak szyfrowania powoduje ujawnienie informacji, które następnie mogą być wykorzystane do przeprowadzenia kolejnych ataków. Przykładowo: cenną informacją, z punktu widzenia atakującego, jest wybrany algorytm szyfrowania używany przez dane urządzenie czy liczba aktywnych asocjacji bezpieczeństwa dla danej stacji.

Problemem może być też brak możliwości sprawdzenia integralności danych użytkowych przy wyborze niektórych algorytmów szyfrowania. Pozwala to na przeprowadzenie ataków odmowy usługi polegających na zalaniu stacji pakietami wygenerowanymi przez atakującego. Bez sprawdzenia integralności wszystkie takie pakiety będą poddawane rozszyfrowywaniu i interpretacji, co pochłonie zasoby atakowanego urządzenia.

Podsumowanie

Sieci WiMAX wydają się bardzo ciekawą alternatywą zapewniającą łączność o parametrach pośrednich między sieciami WiFi a 3G. Obecnie zastosowanie sieci wykorzystujących technologię WiMAX powinno rozwiązać problem ostatniej mili, zwłaszcza na terenach słabo zurbanizowanych. Wprowadzenie rozwiązań takich jak możliwość szyfrowanej komunikacji typu multicast czy mechanizm handover oraz jej dostępne pasmo umożliwią wykorzystanie w przyszłości tych sieci do dostarczania materiałów multimedialnych na urządzenia mobilne.

Na szczególną uwagę zasługuje bardzo poważne i przemyślane podejście do bezpieczeństwa. Wydaje się, że sieci WiMAX pozwolą na budowanie w pełni bezpiecznych sieci radiowych. Na pewno nie grozi nam sytuacja z początków wdrażania sieci WiFi, kiedy okazało się że pierwsze standardy nie zapewniały oczekiwanego poziomu bezpieczeństwa, a kolejne rozwiązania były jedynie łatami bądź dodatkami. W sieciach WiMAX funkcje zapewniające bezpieczne korzystanie z sieci są integralną częścią najważniejszych protokołów.

Krzysztof Cabaj[1,3]
Wojciech Mazurczyk[2,3]
Krzysztof Szczypiorski[2,3]

1) Instytut Informatyki, Politechnika Warszawska
2) Instytut Telekomunikacji, Politechnika Warszawska
3) SecGroup.PL – Network Security Group, Politechnika Warszawska

Literatura:

[1] IEEE 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz Band.
[2] IEEE 802.11g-2003 Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band.
[3] IEEE 802.11i-2004 Amendment 6: Medium Access Control (MAC) Security Enhancements.
[4] IEEE 802.16a-2004 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.
[5] IEEE 802.16e-2005 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.
[6] K. Szczypiorski (kier.), K. Cabaj, I. Margasiński: *Analiza zagrożeń i ochrona danych w sieciach bezprzewodowych,* Instytut Telekomunikacji PW na zlecenie Instytutu Łączności w ramach Programu Wieloletniego Rozwój Telekomunikacji i Poczty w Dobie Społeczeństwa Informacyjnego, Warszawa, 2005.
[7] K. Cabaj, W. Mazurczyk, K. Szczypiorski: *Zarządzanie kluczami w sieciach WiMAX*, materiały XI Krajowej Konferencji Zastosowań Kryptografii Enigma 2007, Warszawa, 23–25 maja 2007 r.
[8] M. Dworkin: *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B*, maj 2005.
[9] B. Aboba, L. Blank, J. Vollbrecht: *Extensible Authentication Protocol (EAP), Request for Comments: 3748*, czerwiec 2004.
[10] H. Krawczyk, M. Bellare, R. Canetti, HMAC: *Keyed-Hashing for Message Authentication, Request for Comments: 2104,* luty 1997.

NOVUS®

Profesjonalne rozwiązanie dla systemów CCTV

CAMA-I

zaawansowane kamery szybkoobrotowe

- zoom całkowity: do 312 x
- mechaniczny filtr podczerwieni (modele dzień/noc)
- wysoka rozdzielczość: do 570 TVL
- czułość: od 0.0003 lx/F=1.6 (DSS)
- 4 trasy obserwacji, 240 presetów, 8 stref prywatności
- zintegrowane wejścia alarmowe
- programowalna funkcja parkowania
- protokoły sterowania: Novus-C, Novus-C1, Pelco-P, Pelco-D
- szeroki wybór akcesoriów do montażu

Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

artykuł sponsorowany

Kamery szybkoobrotowe CAMA-I

Kamera szybkoobrotowa w ostatnim czasie przeszła głęboką metamorfozę. Wzrosły jej funkcjonalność i znaczenie w systemach bezpieczeństwa. W związku z powyższym warto przyjrzeć się możliwościom najnowszej generacji kamer szybkoobrotowych z serii CAMA-I. Do serii kamer szybkoobrotowych CAMA-I należą cztery modele:

1. NVC-SD22C – kolorowa (zoom 22x, przetwornik CCD 1/4" Super-HAD SONY);
2. NVC-SD18DNA – typu dzień/noc (zoom 18x, przetwornik CCD 1/4" ExViewHAD SONY);
3. NVC-SD22DN – typu dzień/noc (zoom 22x, przetwornik CCD 1/4" Super-HAD SONY);
4. NVC-SD26DN – typu dzień/noc (zoom 23x przetwornik CCD 1/4" ExViewHAD).

Wszystkie modele w serii wyglądają identycznie i mają te same funkcje. Różnią się jedynie zastosowanym modułem kamerowym i, tym samym, ustawieniami automatyki ekspozycji. Zastosowane przetworniki CCD 752 (H) x 582 (V) pikseli pozwalają na generacje obrazu wideo o wysokiej rozdzielczości 480 linii telewizyjnych w trybie kolorowym oraz 570 linii w trybie monochromatycznym. Zmiany ogniskowej w szerokim zakresie (dla modelu NVC-SD26DN w granicach 3,5–91,0 mm) umożliwiają zarówno obserwacje szerokich planów (poziomy kąt widzenia 54,2°), jak i realizację dużych zbliżeń (poziomy kąt widzenia 2,2°). Oprogramowanie kamery pozwala również na użycie 10–12-krotnego (w zależności od modelu) zoomu cyfrowego. Umożliwia to uzyskanie nawet 312-krotnych zbliżeń.

Kamera może być sterowana między innymi za pomocą protokołów NOVUS-C, Pelco-D i Pelco-P. Dla powyższej grupy protokołów kamera posiada funkcje autodetekcji, co pozwala na zmianę protokołu sterowania bez konieczności ingerencji w ustawienia przełączników w samej kamerze. Główny moduł kamery przystosowany jest do bezpośredniego montażu na płaskiej powierzchni (np. na suficie). W celu montażu w suficie podwieszanym należy zastosować dodatkowo zestaw NVH-SDHKIT. Obudowy NVH-SD30EH i NVH-SD10I do montażu sufitowego lub ściennego (w komplecie znajduje się zarówno wysięgnik ścienny, jak i sufitowy) są wykonane z aluminium, stali i tworzywa sztucznego. Posiadają one stopień ochrony IP66, co zapobiega przed wnikaniem do wnętrza pyłu i wody, a przy prawidłowym montażu pozwala na ich stosowanie w warunkach silnego zapylenia i oddziaływania strumieni wody. Obudowa NVH-SD30EH jest dodatkowo wyposażona w ochronę przeciwsłoneczną, która zabezpiecza moduł przed przegrzaniem. W obudowie zastosowano grzałkę o poborze mocy 50 W i radiator oraz zespół dwóch wentylatorów (pobór mocy 6 W), poprawiających cyrkulację powietrza. Pozwala to na utrzymanie wymaganej podczas pracy modułu kamerowego temperatury (0°C do +50°C), przy temperaturach otoczenia od -45°C do +50°C. Wykonany z wysokiej jakości plastiku (akrylu) klosz dolny gwarantuje wysoką odporność na udary mechaniczne.

Seria kamer szybkoobrotowych serii CAMA-I, w szczególności modele typu dzień/noc, jest przeznaczona do pracy w warunkach słabego oswietlenia. Sprawdza się zwłaszcza w systemach monitoringu wizyjnego miast, które stawiają przed kamerami najwyższe wymagania w zakresie niezawodności elementów mechanicznych i optycznych oraz odporności na niekorzystne i zmienne warunki atmosferyczne.

Niewielkie wymiary i masa modułu kamerowego gwarantują dużą wytrzymałość mechaniczną oraz prędkość przemieszczania się modułu kamerowego nawet do 380°/s dla ujęć programowych (presetów).

Wysoka czułość modułów kamerowych wynika z zastosowania najwyższej jakości przetworników CCD oraz możliwości wydłużenia czasu ekspozycji nawet do 1 sekundy. Gdy warunki oświetlenia pogarszają się, kamery przechodzą z trybu kolorowego w monochromatyczny (zdejmują mechaniczny filtr podczerwieni), a następnie kamera wydłuża czas ekspozycji. Pozwala to na osiągniecie czułości rzędu dziesięciotysięcznych części luksa, ale należy pamiętać, że tryb pracy migawki (1 s) zapewni jedynie poprawne zobrazowanie elementów statycznych obserwowanej przez kamerę sceny. Natomiast obiekty poruszające się, które dla użytkownika systemu maja największą wartość informacyjną, mogą pozostać zamazane, a tym samym niemożliwe będzie wykorzystanie zarejestrowanego materiału jako pełnowartościowego dowodu. Ustawień kamer dokonuje się za pomocą wyświetlanego na ekranie monitora przejrzystego menu, dostępnego m.in. w języku polskim i angielskim.

Automatyzacja procesu obserwacji jest w kamerze realizowana poprzez funkcje automatycznego skanowania, ujęć programowych, patroli oraz tras automatycznego skanowania. W kamerach CAMA-I można zaprogramować ujęcia programowalne, które pozwalają na szybką i sprawną obsługę urządzenia. Kamery pozwalają na zaprogramowanie maksymalnie 240 presetów i czterech tras obserwacji. Trasa obserwacji to ciąg zapamiętanych funkcji (uchył, obrót,

przybliżenie itp.). Maksymalny czas wszystkich tras wynosi 240 s i może być dowolnie dzielony pomiędzy poszczególne trasy. Połączenie powyższych cech umożliwia funkcja patrolu. Jest to schemat obserwacji składający się z nawet 300 elementów (presetów, tras obserwacji, funkcji automatycznego skanowania oraz samych funkcji patrolu). Dwa 12-stykowe bloki złączy alarmowych, znajdujące się u podstawy modułu kamerowego, pozwalają na zbudowanie wokół kamery szybkoobrotowej podsystemu bezpieczeństwa, złożonego z czujek ruchu oraz elementów peryferyjnych, np. halogenów, syren itp. Do alarmu można przypisać dowolnie wybrany preset, trasę obserwacji, funkcję automatycznego skanowania lub patrol. Po wystąpieniu sygnału alarmowego na jednym z ośmiu wejść kamera realizuje zaprogramowaną funkcję.

Zintegrowane kamery szybkoobrotowe serii CAMA-I mają możliwość nadania nazw 16 strefom ograniczonym zdefiniowanymi azymutami. Nazwy stref mogą być, obok wartości azymutu, elewacji, nazwy i numeru kamery, wyświetlane na ekranie monitora, ułatwiając operowanie kamerą. Włączenie funkcji krańców obserwacji spowoduje, że kamera będzie poruszać się jedynie w zaprogramowanych granicach, przy ręcznym sterowaniu. W przypadku występowania w nadzorowanej strefie miejsc wymagających specjalnego potraktowania, ze względu na konieczność zachowania prywatności można zastosować funkcję maskowania wybranych obszarów. Jest ona szczególnie pożądana w systemach monitoringu miejskiego, ze względu na potrzebę zapewnienia ochrony prywatności obywateli. Zintegrowane kamery kopułowe serii CAMA-I mają możliwość ustawienia ośmiu dynamicznych stref prywatności.

Włączenie funkcji parkowania w kamerze pozwala jej, po upływie określonego czasu braku aktywności ze strony operatora, samoczynnie przystąpić do realizacji określonej funkcji (preset, patrol, automatyczne skanowanie, trasa obserwacji). Czas opóźnienia, po którym następuję automatyczny powrót do pozycji wyjściowej, może być zmieniany w przedziale od 10 do 240 s. W przypadku zaniku, a następnie powrotu zasilania, kamera podejmie ostatnią realizowaną czynność. Gwarantuje to, że w przypadku braku ingerencji operatora w działanie systemu kamera będzie realizowała postawione przed nią zadania.

Wydaje się, że znaczenie kamer szybkoobrotowych w systemach monitoringu wizyjnego będzie nadal wzrastać, choć nie wszędzie istnieje potrzeba ich stosowania. W miarę zwiększania się ich możliwości i spadku cen będą stosowane również w prostych systemach. Dostępna obecnie możliwość sterowania nimi przez Internet znacznie rozszerza ich funkcjonalność i sprawia, że są wartościowym i pożądanym uzupełnieniem stacjonarnych systemów obserwacyjnych. W związku z tym należy oczekiwać, że coraz częściej będą nam towarzyszyć na ulicy, w sklepie, pracy czy na stadionie.

Patryk Gańko
Novus

PROTECTOR

System Depozytariuszy Kluczy

ProxSafe FLEXX

Obudowa o wysokości *24U*
max 128 kluczy

- Obudowa wykonana ze stali (opcja: szkane lub stalowe przednie dzwi)
- 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 w pełni kompatabilnym z kartami/brelokami obsługującymi większość światowych formatów kart.
- 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 umożliwiające: pełną kontrolę nad depozytariuszem, raportowanie pobieranych/zdawanych kluczy, możliwość tworzenia użytkowników, grup kluczy i użytkowników, multiklient, zdalne sterowanie odblokowaniem kluczy, wysyłanie raportów na odres e-mail
- Możliwość zarządzania 32 skrzynkami (1024 kluczy) z poziomu jednego terminala sterującego
- Sterowanie - karta, karta + pin kod, pin kod

Obudowa o wysokości ***12U***
max 64 klucze

Obudowa o wysokości ***6U***
max 32 klucze

www.protector-polska.pl

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

biuro@protector-polska.pl

C & C

TKH GROUP

znamy lepsze sposoby na ochronę...

SHC-730

- Profesjonalna kamera dualna
- Przetwornik CCD 1/3"
- System SVIII z WDR
- Czułość 0,05 Lx @ F1.2 w trybie kolorowym
- 126 razy rozszerzony zakres dynamiki
- Rozdzielczość 520 TVL (tryb kolor), 570 TVL (tryb czarno-biały)
- Najlepsze osiągi przy słabym oświetleniu

STM-19LV

- Rozdzielczość 1280 x 1024 @ 75 Hz
- Wysoki współczynnik kontrastu 700:1
- Wysoka jasność: 300 cd/m²
- Czas reakcji 8 ms
- Złącze BNC
- Złącze S-Video
- Wejścia RGB
- Wbudowane głośniki
- Ekran ochronny

SAMSUNG TECHWIN

Autoryzowany dystrybutor Samsung Techwin w Polsce:
C&C Partners - Leszno

www.samsungcctv.ccpartners.pl

Przemysłowy system komunikacji wewnętrznej

artykuł sponsorowany

Rola człowieka w nowoczesnym przedsiębiorstwie, pomimo coraz większej automatyzacji, nadal pozostaje nie do przecenienia. Dlatego też szczególnego znaczenia nabiera zapewnienie pracownikom szybkiego, sprawnego i niezawodnego systemu komunikacji, dzięki któremu nie tylko zostanie poprawiona efektywność, ale wzrosną także komfort i bezpieczeństwo pracy.

Spośród dostępnych na rynku technologii komunikacyjnych w trudnych warunkach przemysłowych, szczególnie dobrze sprawdzają się systemy typu interkom austriackiej firmy Commend, której przedstawicielem w Polsce jest firma C&C Partners Telecom

System Commend – elastyczność i funkcjonalność

Wymagania stawiane systemom komunikacyjnym przez współczesny przemysł są bardzo wysokie, dlatego też firma Commend stworzyła nowoczesny i elastyczny system łączności wewnętrznej cechujący się dużą niezawodnością i unikatowymi rozwiązaniami takimi jak technologie *Open Duplex* czy *Intercom over IP*.

System przemysłowy Commend ma budowę modułową, co pozwala na tworzenie zarówno małych, jak i wielkich, składających się z kilku tysięcy stacji, sieci komunikacji wewnętrznej. Architektura gwiazdy zapewnia dużą niezawodność, a dwużyłowe okablowanie ogranicza koszty instalacji systemu. Dostępna duża liczba kart rozszerzeń pozwala na rozbudowę o dodatkowe funkcje, a także integracje z innymi systemami funkcjonującymi na terenie przedsiębiorstwa (np. z analogowymi i cyfrowymi [ISDN] centralami telefonicznymi czy z systemami radiotelefonicznymi). Dzięki dużemu wyborowi stacji i ich modułowej budowie możliwe jest ścisłe dopasowanie do różnych warunków i lokalizacji, nie wyłączając stref zagrożonych wybuchem.

Właściwie wszystkie funkcje systemu są dostępne z poziomu programu konfiguracyjnego, dzięki czemu możliwe jest szybkie i proste nadzorowanie systemu z jednego miejsca oraz adaptowanie go do zmieniających się wymagań.

Przemysłowe stacje interkomowe

Specyfika przemysłowa, a w szczególności hałas i niekorzystne warunki otoczenia, stawiają wysokie wymagania, którym starali się sprostać konstruktorzy firmy Commend. Opracowane przez nich stacje serii EE8000 charakteryzują się wieloma ciekawymi rozwiązaniami. Przede wszystkim stacje te mają w pełni modułową budowę, dzięki czemu można ściśle dopasować parametry do wymagań. Dzięki zastosowaniu technologii DSP możliwa jest programowa zmiana m.in. czułości mikrofonu w zakresie aż 30 dB oraz wykorzystanie zalet technologii Open Duplex. Wbudowany wzmacniacz klasy D o mocy 25 W zapewnia bardzo dobrą słyszalność nawet przy bardzo dużym natężeniu hałasu. Duże przyciski, z dwukolorowym podświetlaniem LED, ułatwiają korzystanie ze stacji, nawet w przypadku stosowania rękawic ochronnych. Każdy z przycisków może być dowolnie skonfigurowany, a jedną stację można wyposażyć w 50 swobodnie programowalnych klawiszy.

Przemysłowe systemy Commend doskonale sprawdzają się nawet w ekstremalnych warunkach

Obudowa stacji wykonana została z poliestru wzmocnionego włóknem szklanym w dobrze widocznym kolorze pomarańczowym i charakteryzuje się klasą szczelności IP65.

System Commend – praktyczne możliwości

Poza stroną techniczną także bogata funkcjonalność jest atutem przemysłowych systemów Commend. Do najważniejszych zalet należy zaliczyć:

- szybkie połączenie punkt–punkt. Wciśnięcie jednego przycisku inicjuje połączenie,
- rozmowę prowadzoną w „naturalny" sposób (*Open Duplex*) w trybie głośnomówiącym, nawet przy dużym hałasie,
- rozbudowany tryb wywołań grupowych, dzięki któremu możliwe jest zastąpienie systemów PA (powiadamiania publicznego, od ang.: *Public Address*),
- możliwość wprowadzenia do systemu zewnętrznych sygnałów audio, np. wybranych stacji radiowych lub zakładowego radiowęzła,
- tryb konferencyjny umożliwiający stałą łączność pomiędzy wybranymi stacjami, np. wzdłuż jednej linii produkcyjnej,
- możliwość integracji z innymi systemami, np. SSP, w celu automatycznego rozgłaszania komunikatów (np. o ewakuacji na wypadek pożaru),
- możliwość sterowania innymi elementami z poziomu stacji interkomowej (np. załączaniem oświetlenia, otwieraniem bram, barier itp.).

W przypadku rozbudowanych systemów możliwe jest zastosowanie dedykowanego oprogramowania wizualizacyjnego lub integracja z istniejącymi już w danym obiekcie systemami SCADA, nadzorującymi zbieranie danych i sterowanie procesem technologicznym lub produkcyjnym (z ang.: *Supervisory Control And Data Acquisition*).

Należy też wspomnieć, że rozwiązania firmy Commend charakteryzują się wielopoziomową samokontrolą. Wszystkie linie sygnałowe są stale monitorowane, a dodatkowe mechanizmy nadzoru, takie jak audiomonitoring i system kontroli układu mikrofon–głośnik, pozwalają na natychmiastowe wykrycie najdrobniejszej usterki i zgłoszenie jej.

Podsumowanie

W dzisiejszym przemyśle system łączności to nie tylko sposób na komunikację, to także skuteczny środek na zwiększenie efektywności i wzrost wydajności, oraz, co równie istotne, inwestycja w bezpieczeństwo pracownika. Dlatego ważne jest, aby stosowane rozwiązania charakteryzowały się funkcjonalnością, niezawodnością i intuicyjnością obsługi. Z pewnością przemysłowe systemy Commend spełniają wszystkie te kryteria.

Open Duplex – technologia oparta na cyfrowym przetwarzaniu sygnału, zapewniająca możliwość jednoczesnego mówienia i słuchania bez konieczności ręcznej kontroli kierunku rozmowy. Dodatkowa funkcja eliminacji szumu otoczenia pozwala na wygodną konwersacje nawet przy dużym hałasie.

Intercom over IP – rozwiązanie pozwalające na podłączenie stacji interkomowej bezpośrednio do sieci typu Ethernet i komunikacji z serwerem systemu Commend za pomocą protokołu IP. Umożliwia to budowanie rozproszonego systemu łączności z wykorzystaniem globalnego zasięgu Internetu.

Przemysław Kaźmierczak
C&C Partners Telecom
www.commend.pl

PRT 12

zewnętrzny czytnik RFID/PIN

Czytniki serii PRT

- Identyfikacja zbliżeniowa oraz PIN
- Technologia EM 125 kHz oraz Mifare
- Praca autonomiczna lub jako czytnik podległy kontrolerowi
- Interfejsy Wiegand oraz Magstripe (Clock & Data)
- Praca w warunkach zewnętrznych (IP65)
- Obudowa jasnoszara lub ciemna

RACS

ROGER ACCESS CONTROL SYSTEM

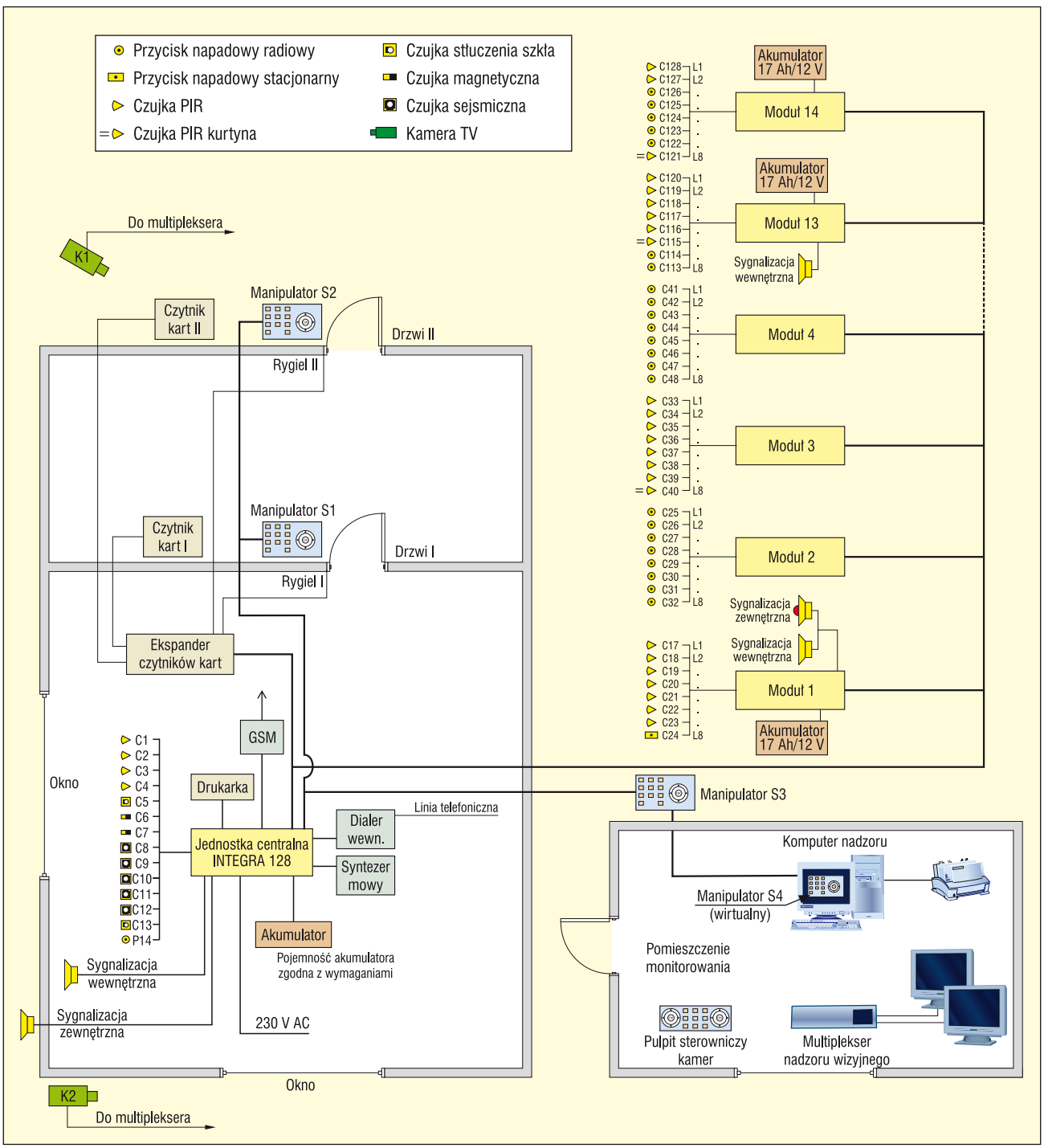
roger®

www.roger.pl

Analiza niezawodnościowa
złożonego systemu bezpieczeństwa dla obiektu o specjalnym przeznaczeniu

Wprowadzenie

Niniejszy artykuł przedstawia kolejne wnioski z przeprowadzonych przez autorów badań dotyczących elektronicznych systemów bezpieczeństwa o różnych stopniach komplikacji. Badano procesy eksploatacyjno-niezawodnościowe rozproszonych systemów bezpieczeństwa, ze szczególnym uwzględnieniem tych dotyczących wyższych kategorii zagrożeń (Z3 i Z4) oraz klasyfikowanych jako SA3 i SA4. Nacisk położono na obiekty o specjalnym znaczeniu. Zwykle posiadają one bardzo rozbudowane elektroniczne systemy bezpieczeństwa o charakterze rozproszonym, obejmujące również telewizję dozorową wysokiej rozdzielczości z rejestracją na dyskach twardych, kontrolę dostępu – realizowaną niezależnie lub opcjonalnie stanowiącą fragment centrali systemu



Rys. 1. Schemat blokowy roproszonego systemu bezpieczeństwa

sygnalizacji włamania i napadu (SSWiN), system przeciwpożarowy (niezależny lub w ograniczonym zakresie stanowiący również fragment ww. centrali). Bardzo często elektroniczne systemy bezpieczeństwa są powiązane z systemami mechanicznymi (drzwi, okna a w nich szyby o klasach od P3 do P7, rygle drzwiowe, trzymaki magnetyczne itp.).

W *Zabezpieczeniach nr 1/2 (41/42)* z roku 2005 autorzy przeanalizowali struktury niezawodnościowe w rozproszonych systemach bezpieczeństwa, podając schematy niezawodnościowe spotykane w praktyce oraz przedstawili w postaci grafów relacje zachodzące w elektronicznych systemach bezpieczeństwa. Przeprowadzono również analizę matematyczną w postaci równań, za pomocą których można obliczyć prawdopodobieństwo przebywania systemów w ściśle określonych stanach eksploatacyjno-niezawodnościowych. Były to jednak propozycje teoretyczne wymagające podbudowy praktycznej.

Takie badania autorzy zaczęli prowadzić, poczynając od 2005 roku: zbierali dane eksploatacyjno-niezawodnościowe z bardzo wielu elektronicznych systemów bezpieczeństwa o skomplikowanej budowie (opracowano specjalne karty do zbierania danych o uszkodzeniach). W trakcie tych działań napotykali na wiele problemów eksploatacyjno-niezawodnościowych. Dotyczyły one zwłaszcza systemów rozproszonych zaprojektowanych i zrealizowanych w obiektach o szczególnym przeznaczeniu (ze zrozumiałych względów nie można podać, jakie to są obiekty).

W *Zabezpieczeniach nr 1 (47)* z 2006 roku autorzy przedstawili schemat blokowy rozproszonego systemu bezpieczeństwa zaprojektowanego z wykorzystaniem jednostki mikroprocesorowej typu INTEGRA 64. Analizując już rzeczywisty (trudny ze względu na swoje przeznaczenie) obiekt, zbudowano schemat niezawodnościowy elektronicznego systemu bezpieczeństwa interpretujący ww. schemat ideowy. Następnie zbudowano model eksploatacyjno-niezawodnościowy w postaci grafu przejść. Wykorzystano również skomplikowany aparat matematyczny umożliwiający obliczenie przebywania systemu bezpieczeństwa w określonym stanie eksploatacyjnym (np. przejście ze stanu pełnej zdatności do stanu zagrożenia bezpieczeństwa). Wtedy nasunął się istotny wniosek: niezawodność rozproszonych systemów bezpieczeństwa (zwanych też systemami nadzoru) należy kształtować już na etapie projektowania oraz praktycznej realizacji systemu. Można ją również korygować podczas eksploatacji (np. rozbudowa już istniejącego systemu), przez odpowiednie zmiany w strukturze niezawodnościowej, choć niektóre bloki systemu są na taką korektę odporne.

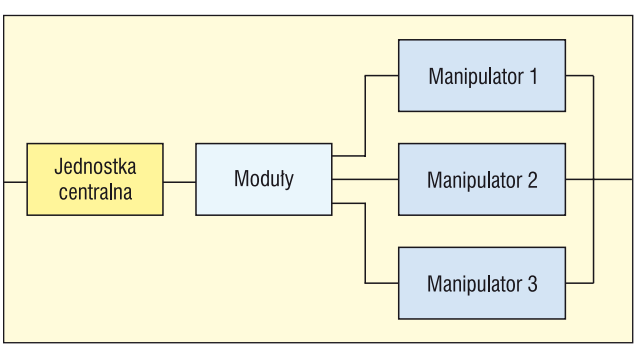
Syntetyczny opis praktycznego rozproszonego systemu bezpieczeństwa

Na rys. 1. przedstawiono zmodyfikowany rozproszony system bezpieczeństwa, znacznie bardziej rozbudowany, niż wspomniany powyżej. Modyfikacja wynikała z potrzeb obiektu specjalnego znaczenia. Wprowadzono jednostkę mikroprocesorową INTEGRA 128 o 128 liniach wejściowych, dobudowano wiele modułów rozszerzających (na dwóch magistralach jest ich 14). Znacznie rozbudowano pomieszczenie ochrony, w którym system bezpieczeństwa jest monitorowany. Tam też znajduje się komputer nadzorujący pracę SSWiN i 16-wejściowy multiplekser cyfrowy z rejestracją zdarzeń na dyskach twardych. Również w tym pomieszczeniu znajdują się urządzenia, zapewniające dwie drogi monitorowania: telekomunikacyjną i radiową. Elektroniczny system bezpieczeństwa został wyposażony w cztery manipulatory LCD, w tym jeden wirtualny. Wynika to z organizacji obiektu. Z pomieszczenia ochrony są sterowane zarówno szybkoobrotowe głowice kamer TV, jak i zastosowane w kamerach obiektywy o zmiennej ogniskowej. Rezerwowe źródła zasilania (akumulatory) w przypadku awarii zasilania zasadniczego (230V) umożliwiają pracę systemu bezpieczeństwa przez minimum 72 godziny. Kamery CCTV współpracują z oświetlaczami podczerwieni o sporym zasięgu (od 8 do 25 m).

Warto również wspomnieć o mechanicznych zabezpieczeniach zaproponowanych i zrealizowanych w obiekcie rzeczywistym specjalnego znaczenia. Są to okna posiadające szyby kategorii P5. W pomieszczeniach widocznych na rys. 1. zostały zainstalowane atestowane stalowe drzwi (I i II) z atestowanymi zamkami. Wprowadzono rygle elektromagnetyczne sterowane czytnikami kart (z rejestracją wejścia/wyjścia). System kontroli dostępu, który jest zrealizowany na tej samej jednostce mikroprocesorowej, ze względów bezpieczeństwa współpracuje z systemem przeciwpożarowym. Ściany, podłogi, sufity w pomieszczeniach są chronione czujkami sejsmicznymi klasy S. Podobnymi czujkami są chronione sejfy pancerne.

Model eksploatacyjno-niezawodnościowy rzeczywistego systemu bezpieczeństwa

Na rys. 2. przedstawiono model eksploatacyjno-niezawodnościowy, który powstał w wyniku analizy rzeczywistego elektronicznego systemu bezpieczeństwa przedstawionego na rys. 1. Ze względu na duży stopień komplikacji rzeczywistego systemu bezpieczeństwa zastosowano niezbędne



Rys. 2. Schemat niezawodnościowy systemu bezpieczeństwa (model interpretujący rys. 1)

uproszczenia, takie, które nie wypaczą logiki badań.

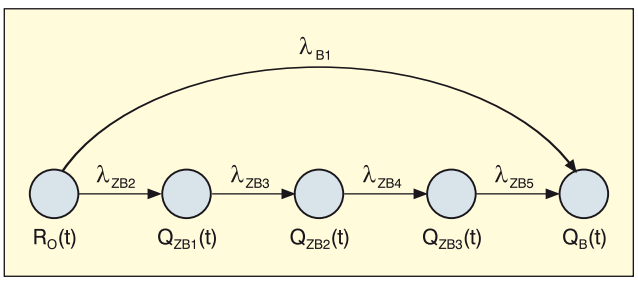
14 modułów rozszerzających zostało przedstawionych w postaci jednego bloku i dołączonych do bloku jednostki mikroprocesorowej (centralnej). Do magistral zostały ze względów logistycznych dołączone cztery manipulatory LCD, w tym jeden wirtualny. Tak zbudowany schemat eksploatacyjno-niezawodnościowy stanowi tzw. mieszany model niezawodnościowy (trudny do analizy matematycznej). Można więc tu mówić o problemie nadmiarowości. Warto przypomnieć, że z punktu widzenia eksploatacji i niezawodności można wyróżnić następujące rodzaje nadmiarowości:

– nadmiar strukturalny,
– nadmiar funkcjonalny,
– nadmiar parametryczny,
– nadmiar informacyjny,
– nadmiar wytrzymałościowy,
– nadmiar czasowy,
– nadmiar elementowy.

Analizując szczegółowo schemat przedstawiony na rys. 1. i jego uproszczony schemat niezawodnościowy (rys. 2.), można stwierdzić, że mogą mieć miejsce wszystkie ww. nadmiary.

Jednak dla badań szczególnie istotne są dwa: strukturalny (przejście na rezerwowe źródło zasilania w przypadku awarii źródła zasadniczego) i funkcjonalny (kilka manipulatorów LCD i jeden wirtualny). Ten ostatni nadmiar funkcjonalny jest bardzo ważny ze względu na logikę i procedury obowiązujące w tego typu obiektach specjalnego znaczenia.

W wyniku analizy blokowego schematu niezawodnościowego (uproszczonego) autorzy zaproponowali graf relacji zachodzących w rozproszonym systemie bezpieczeństwa. Relacje te dla rzeczywistego obiektu zostały przedstawione na rys. 3.



Rys. 3. Relacje zachodzące w systemie bezpieczeństwa (na podstawie rys. 2), gdzie:
$R_O(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie pełnej zdatności,
$Q_{ZB}(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa,
$Q_B(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zawodności bezpieczeństwa,
λ_{B1} – intensywność przejść central i modułów,
λ_{ZB2}, λ_{ZB3}, λ_{ZB4}, λ_{ZB5} – intensywność przejść manipulatorów

Szczegółowy mechanizm przejść z określonych stanów został opisany wcześniej (*Zabezpieczenia nr 1/2 (41/42)*, 2005 rok).

Jeżeli dokona się przekształceń matematycznych (niestety, bardzo skomplikowanych), można otrzymać zależności, które pozwolą wyznaczyć wartości prawdopodobieństw przebywania rozważanego (rzeczywistego) elektronicznego systemu bezpieczeństwa w odpowiednich stanach:

– pełnej zdatności R_0

$$R_0(t) = e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}$$

– zagrożenia bezpieczeństwa Q_{ZB1}

$$Q_{ZB1}(t) = \lambda_{ZB2} \cdot \left[\frac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t} - e^{-\lambda_{ZB3}\cdot t}}{\lambda_{ZB3} - \lambda_{B1} - \lambda_{ZB2}} \right]$$

– zagrożenia bezpieczeństwa Q_{ZB2}

$$Q_{ZB2}(t) = \lambda_{ZB2} \cdot \lambda_{ZB3} \cdot \left[\frac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})} - \frac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot(\lambda_{ZB3}-\lambda_{ZB4})} + \frac{e^{-\lambda_{ZB4}\cdot t}}{(\lambda_{ZB3}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})} \right]$$

– zagrożenia bezpieczeństwa Q_{ZB3}

$$Q_{ZB3}(t) = \lambda_{ZB2} \cdot \lambda_{ZB3} \cdot \lambda_{ZB4} \cdot \left[\frac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})} - \frac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{ZB5}-\lambda_{ZB3})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot(\lambda_{ZB3}-\lambda_{ZB4})} + \frac{e^{-\lambda_{ZB4}\cdot t}}{(\lambda_{ZB5}-\lambda_{ZB4})\cdot(\lambda_{ZB4}-\lambda_{ZB3})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})} - \frac{e^{-\lambda_{ZB5}\cdot t}}{(\lambda_{ZB5}-\lambda_{ZB3})\cdot(\lambda_{ZB5}-\lambda_{ZB4})\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})} \right]$$

– zawodności bezpieczeństwa Q_B

$$Q_B(t) = \frac{\lambda_{B1}}{\lambda_{B1}+\lambda_{ZB2}} \cdot \left[1 - e^{-(\lambda_{B1}+\lambda_{ZB2})t}\right] + \lambda_{ZB2} \cdot \lambda_{ZB3} \cdot \lambda_{ZB4} \cdot \lambda_{ZB5} \cdot \left[\frac{-e^{-(\lambda_{B1}+\lambda_{ZB2})t}}{(\lambda_{B1}+\lambda_{ZB2})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})} + \frac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot\lambda_{ZB3}\cdot(\lambda_{ZB3}-\lambda_{ZB4})\cdot(\lambda_{ZB5}-\lambda_{ZB3})} - \frac{e^{-\lambda_{ZB4}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{ZB3}-\lambda_{ZB4})\cdot\lambda_{ZB4}\cdot(\lambda_{ZB5}-\lambda_{ZB4})} + \frac{e^{-\lambda_{ZB5}\cdot t}}{\lambda_{ZB5}\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})\cdot(\lambda_{ZB5}-\lambda_{ZB4})\cdot(\lambda_{ZB5}-\lambda_{ZB3})} + \frac{1}{(\lambda_{B1}+\lambda_{ZB2})\cdot\lambda_{ZB3}\cdot\lambda_{ZB4}\cdot\lambda_{ZB5}} \right]$$

Oznaczenia w powyższych zależnościach są następujące:
t – czas,
λ_{B1} – intensywność przejść central i modułów,
λ_{ZB} – intensywność przejść manipulatora LCD

Obliczenia wskaźników niezawodnościowo-eksploatacyjnych

a) czas obserwacji systemu – 1 rok = 8760 h.
b) liczba badanych systemów: 100 (takich jak na rys. 1. lub podobnych)
c) liczba uszkodzonych manipulatorów odpowiednio w gałęziach modelu niezawodnościowego: 4, 3, 2, i 1.
d) liczba uszkodzonych modułów i central (łącznie).

Otrzymane wartości prawdopodobieństw przebywania systemu w:
– stanie pełnej zdatności systemu R_0: 0,9504
– stanie zagrożenia bezpieczeństwa Q_{ZB1}: 0,039195
– stanie zagrożenia bezpieczeństwa Q_{ZB2}: 0,000601
– stanie zagrożenia bezpieczeństwa Q_{ZB3}: 0,000004
– stanie zawodności bezpieczeństwa Q_B: 0,009798

Powyższe wskaźniki zostały wyliczone na podstawie ww. równań z wykorzystaniem autorskiego programu komputerowego Wspomagania Decyzji Niezawodnościowo-Eksploatacyjnych Transportowych Systemów Nadzoru.

Zakończenie i wnioski

Przedstawione wyniki obliczeń wymagają pewnych wyjaśnień. Gdyby przyjąć za ostateczny wynik R_0=0,9504, a więc stan pełnej zdatności elektronicznego systemu bezpieczeństwa,

wynik ten nie byłby satysfakcjonujący. Należy brać jednak pod uwagę, czego dotyczą wskaźniki: QZB1, QZB2, QZB3. Wyliczone wartości dotyczą stanu zagrożenia bezpieczeństwa wynikające z niezdatności kolejnych trzech manipulatorów LCD (w systemie bezpieczeństwa jest ich cztery). Aby więc mieć pełny obraz zdatności elektronicznego systemu bezpieczeństwa przedstawionego na rys. 1., należy przyjąć pewne założenia. Mianowicie:

– wszystkie trzy manipulatory LCD realizują identyczne funkcje,
– podobnie i czwarty manipulator, wirtualny (jednak rozpatrywany rozdzielnie),

Jeśli przyjąć takie założenie, stan pełnej zdatności elektronicznego systemu bezpieczeństwa można wyrazić równaniem:

$$R_{0(całk)}=R_0+Q_{ZB1}+Q_{ZB2}+Q_{ZB3}=$$

$$=0,9504+0,039195+0,000601+0,000004=0,9902$$

Można więc przedstawić warunek wystarczający dla analizowanego elektronicznego systemu bezpieczeństwa obiektu specjalnego przeznaczenia:

$$0,9902 \le R_{0całk.} \le 0,9504$$

Można odczytać, że dla granicy prawostronnej zdatny jest tylko manipulator wirtualny, a dla lewostronnej zdatne są wszystkie. Tak więc w podanym przedziale można przyjąć, że system bezpieczeństwa znajduje się w pełnej zdatności. W trakcie analizy elektronicznego systemu bezpieczeństwa nie były brane pod uwagę wszystkie procedury dotyczące obiektu specjalnego przeznaczenia. W przypadku gdy wszystkie cztery manipulatory są w stanie zawodności bezpieczeństwa (jest to możliwe), analizowany system bezpieczeństwa nie nadaje się do dalszej eksploatacji.

DR INŻ. WALDEMAR SZULC
POLITECHNIKA WARSZAWSKA, WYDZIAŁ TRANSPORTU,
ZAKŁAD TELEKOMUNIKACJI W TRANSPORCIE
WYŻSZA SZKOŁA MENEDŻERSKA W WARSZAWIE, WYDZIAŁ INFORMATYKI

DR INŻ. ADAM ROSIŃSKI
POLITECHNIKA WARSZAWSKA, WYDZIAŁ TRANSPORTU,
ZAKŁAD TELEKOMUNIKACJI W TRANSPORCIE

Literatura:

1. Instrukcje serwisowe systemów: GALAXY, RANKOR, SATEL, DSC, SIEMENS.
2. Będkowski L., Dąbrowski T.: *Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej.* Wojskowa Akademia Techniczna, Warszawa, 2006.
3. Szulc W., Rosiński A.: *Problemy eksploatacyjno-niezawodnościowe rozproszonego systemu bezpieczeństwa,* Zabezpieczenia, nr 1 (47), Warszawa, 2006.
4. Rosiński A.: *Analiza struktur niezawodnościowych w rozproszonych systemach bezpieczeństwa*. Zabezpieczenia nr 1/2 (41/42), Warszawa, 2005.
5. Ważyńska-Fiok K., Jaźwiński J.: *Niezawodność systemów technicznych*, PWN, Warszawa, 1990.

DOSKONAŁA FUNKCJONALNOŚĆ ZA NIESPOTYKANĄ CENĘ

24M.pl

wyłączny przedstawiciel producenta w Polsce

przetestuj
przez 10 dni za darmo

pokrętło jog shuttle

2399 PLN netto

obsługa przez mysz

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

REJX16

REJX4

pokrętło jog shuttle

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

Specyfikacja

zobacz online: **www.24m.pl/rejx4**

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**

Możliwe, że już zostałeś zauważony BX-80N

OCHRONA OBWODOWA – WCZESNE OSTRZEGANIE

Czujkę BX-80N charakteryzuje zaawansowana technologia pasywnej podczerwieni, która w efektywny sposób wykrywa i odstrasza potencjalnego intruza. Jedna czujka gwarantuje ochronę elewacji o długości aż do 24 m, stanowiąc pierwszą linię ochrony obiektu.

Czujkę BX-80N cechuje:

- Unikalna, obustronna strefa detekcji pozwalająca na ochronę okien wzdłuż elewacji budynku.
- Opatentowana technologia „Double Conductive Shielding", wykorzystująca filtrację fal z zakresu światła widzialnego, jak i fal elektromagnetycznych, zapewniająca redukcję fałszywych alarmów do minimum.
- Efektowny, estetyczny design, dzięki któremu czujka doskonale komponuje się z różnymi typami elewacji budynków.

OPTEX

CECHY UŻYTKOWE

Opatentowana technologia „Double Conductive Shielding"

Zastosowane filtry technologii „Double Conductive Shielding", oprócz filtracji fal z zakresu światła widzialnego, posiadają również własności filtracji fal elektromagnetycznych. Pozwala to na skuteczne ekranowanie pyroelementów wrażliwych na działanie zakłóceń elektromagnetycznych, redukując powstawanie fałszywych alarmów, powodowanych przez źródła światła takie jak słońce i reflektory samochodów.

Daleki zasięg detekcji – 24m

Czujka charakteryzuje się długim i wąskim obszarem detekcji – 24m, specjalnie zaprojektowanym do ochrony budynków wzdłuż elewacji.

- **Funkcja ograniczenia zasięgu wykrywania**
  Zasięg detekcji może być regulowany, co pozwala na dopasowanie go do długości elewacji.
- **Funkcja rozróżniania wielkości intruza**
  W czujce zastosowano niezawodną metodę podwójnej detekcji, która zapobiega fałszywym alarmom, wywoływanym przez ptaki lub inne małe zwierzęta. Pole widzenia czujki zostało podzielone na dwa odrębna obszary detekcji: górny i dolny. Alarm wystąpi, jeśli intruz zostanie wykryty w obu obszarach.

Prosta instalacja

Czujka BX-80N jest prosta w instalacji i regulacji – nie ma potrzeby strojenia toru optycznego, co ma miejsce w przypadku instalacji barier podczerwieni. Aby czujka chroniła obie strony elewacji, wystarczy umieścić ją w środkowej części zewnętrznej ściany budynku.

Dźwiękowa sygnalizacja alarmu

Wbudowany sygnalizator z funkcją głośnego ostrzegania o naruszeniu pola detekcji działa odstraszająco na intruza i może powstrzymać go przed kontynuowaniem włamania.

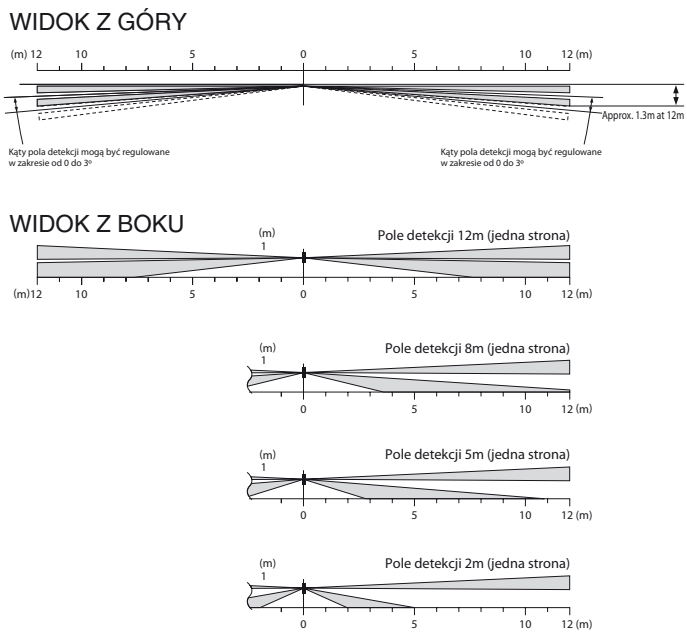
SPECYFIKACJA

	BX 80N
Metoda detekcji	PIR
Zasięg detekcji	24m (po 12m na każdą stronę)
Ilość wiązek	4 (po 2 na każdą stronę)
Czułość	1,6°C przy 0,6 m/s
Wykrywana prędkość ruchu	0,3 - 2,0 m/s
Zasilanie	10 - 28 V⎓
Pobór prądu	38 mA (maks.)
Czas trwania alarmu	2 ± 1 sekundy
Wyjście alarmowe	2 przekaźniki N.C. i N.O. 28V⎓, 0,2A maks. każdy
Styk sabotażowy	N.C., otwarty po zdjęciu obudowy
Czas trwania testu po podaniu zasilania	Około 45 sekund (dioda LED miga)
Głośność sygnalizacji alarmu	około 70dB (w odległości 1 m)
Wskaźnik LED	Miga w czasie testu po podaniu zasilania Wskazuje stan alarmu
Temperatura pracy	-20°C - +50°C
Wilgotność	Do 95%
Odporność na zakłócenia radioelektryczne	20 V/m
Montaż	Na ścianie
Wysokość montażu	0,8 – 1,2 m
Ciężar	400g
Stopień ochrony	IP55

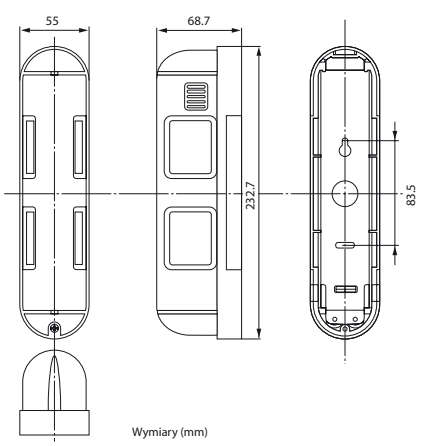
AKCESORIA

MG-1 Osłona metalowa, wandaloodporna

CHARAKTERYSTYKA DETEKCJI



WYMIARY



*Producent zastrzega możliwość zmian w specyfikacji technicznej urządzeń bez wcześniejszego poinformowania.

Wyłączny dystrybutor produktów Optex w Polsce:

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

artykuł sponsorowany

Czujki CX-502, CX-502AM, CX-502AMplus

Kilka ostatnich artykułów zostało poświęconych nowościom w ofercie firmy Optex. Pozostałe produkty tej firmy, obecne na naszym rynku już od jakiegoś czasu, również zasługują na uwagę. Przykładem niech będzie seria wewnętrznych pasywnych czujek podczerwieni (PCP) CX-502.

W instalacjach o wysokim poziomie ochrony stosowanie zwykłych czujek wysokiej klasy nie wystarcza. Powinny one dodatkowo spełniać wiele wymagań, np. posiadać funkcje samokontroli czy zdolność wykrycia prób sabotażu uniemożliwiającego ich prawidłową pracę.

Takie wymagania w pełni spełnia linia produktów CX-502 firmy Optex, głównego producenta czujek alarmowych specjalizującego się w urządzeniach wykorzystujących zjawiska związane z promieniowaniem podczerwonym. Nic więc dziwnego, że również i te produkty należą do ścisłej czołówki dostępnych na rynku urządzeń.

W skład serii wchodzą następujące produkty:
- CX-502 – czujka ruchu klasy C,
- CX-502AM – czujka ruchu klasy S z funkcją antymaskingu,
- CX-502AMplus – czujka ruchu klasy S z funkcją antymaskingu – nowość!

Zastosowane technologie

Jak wszystkie czujki wewnętrzne firmy Optex urządzenia serii CX-502 są wyposażone w podwójne pyroelementy. Posiadają też wysokiej jakości wzmacniacze analogowe. Tor optyczny został wyposażony w filtry światła białego (*Double Conductive Shielding*). Filtry wykonane w tej technologii skutecznie oddzielają promieniowanie podczerwone od innych źródeł promieniowania oraz pełnią rolę ekranu przed zakłóceniami elektromagnetycznymi. Najważniejszym elementem toru optycznego jest soczewka. Precyzja wykonania, powtarzalność parametrów oraz dokładność pozycjonowania względem pyroelementu w gotowej czujce to najważniejsze czynniki decydujące o jakości PCP. Detektory CX-502 to najlepszy przykład pedantycznej wręcz dbałości o szczegóły. Soczewka zastosowana w czujkach CX-502 łączy w sobie zalety soczewek sferycznych (będąc wycinkiem kuli, zapewnia optymalny kąt przejścia promieniowania podczerwonego) i płaskich (niewielkie rozmiary czujek). Projekt każdego elementu soczewki jako osobnego wycinka i złożenie tych wycinków w jednolitą wypukłą powierzchnię (*Offset Spherical Lens*) powoduje, że uzyskana tak spłaszczona soczewka umożliwia konstrukcję czujek o niewielkich rozmiarach. Zastosowanie technologii segmentacji pola widzenia czujki (*Quad Zone Logic*) pozwala wykorzystać efekt zwielokrotnienia sygnału docierającego do pyroelementu. Dzięki tej technologii obiekty duże – wielkości człowieka – generują kilkukrotnie większy sygnał użyteczny niż obiekty małe (zwierzęta mniejsze od człowieka). Niezwykle istotne jest to, że zwielokrotnienie sygnału realizowane jest w torze optycznym, więc nie ma wpływu na poziom szumów pochodzących ze wzmacniaczy.

Czujki serii CX są wyposażone w cyfrową, mikroprocesorową analizę sygnału. Umożliwia to zastosowanie dodatkowych funkcji zwiększających stabilność pracy detektora oraz ograniczenie występowania niepożądanych zjawisk związanych ze zmianami temperatury otoczenia (*Advanced Digital Temperature Compensation*). Algorytm dostosowania czułości detektora do temperatury otoczenia pozwala utrzymać optymalną dynamikę sygnału dla prawidłowej pracy algorytmów detekcyjnych w szerokim spektrum temperatur, zwłaszcza w najbardziej newralgicznym dla PCP zakresie pomiędzy 35°C a 40°C.

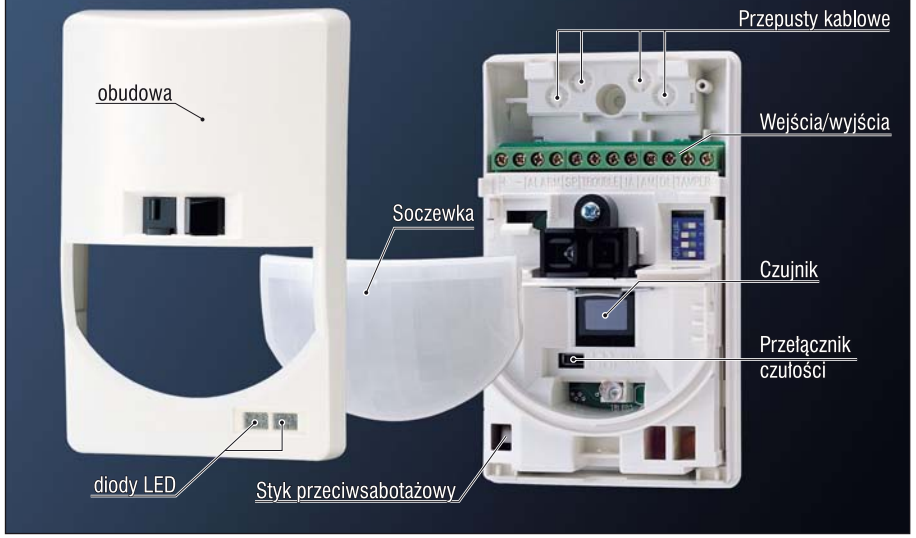
Jak większość czujek alarmowych wyższych klas zabezpieczenia również seria CX-502 została wyposażona w rozwiązania wykluczające sabotaż styków wskutek działania zewnętrznych pól magnetycznych (tzw. *Silent Relay*). Zastosowanie technologii optoelektronicznych i unipolarnych pozwoliło na uzyskanie izolacji elektromagnetycznej układów elektronicznych czujki od obwodów systemu alarmowego. Również obwody zasilania wyposażono w odpowiednie filtry i środki ochrony przeciwprzepięciowej.

Funkcje specjalne dostępne w detektorach klasy S (CX-502AM, CX-502AMplus)

Wieloletnie badania firmy Optex nad przyczynami awarii w PCP doprowadziły do interesujących konkluzji. Otóż okazuje się, że ponad 95% wszystkich uszkodzeń czujek dotyczy toru analogowego oraz analizy sygnału niezależnie od technologii jej wykonania. Niezwykle rzadko występują natomiast awarie spowodowane uszkodzeniem układów formujących sygnały wyjściowe, a uszkodzenia układu optycznego to już pojedyncze przypadki (zresztą łatwo weryfikowane wzrokowo). W związku z tym zdecydowano się wprowadzić funkcję automatycznego, samoczynnego testowania sprawności

czujki (*Self Check*). Czujka co pięć godzin pracy przechodzi w tryb testowy, w czasie którego blokowane jest wyjście alarmowe urządzenia, a na wejście toru analogowego (wyjście pyroelementu) podawany jest sygnał testowy. Brak reakcji czujki na sygnał testowy oznacza uszkodzenie sygnalizowane aktywacją wyjścia T.O. (*Trouble Output*). Test trwa bardzo krótko i w żaden sposób nie jest sygnalizowany na zewnątrz. Samokontrola czujki pozwala wychwycić awarię niemalże w momencie jej wystąpienia, a nie dopiero podczas przeglądu systemu przez pracowników obsługi technicznej. Eliminując czynnik ludzki w ocenie swojej sprawności, czujki serii CX-502 zapewniają wyjątkowo wysoki poziom zabezpieczenia.

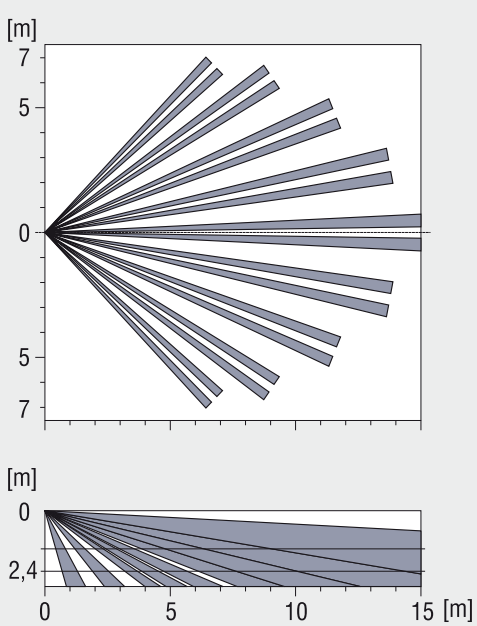
Budowa czujek serii CX-502



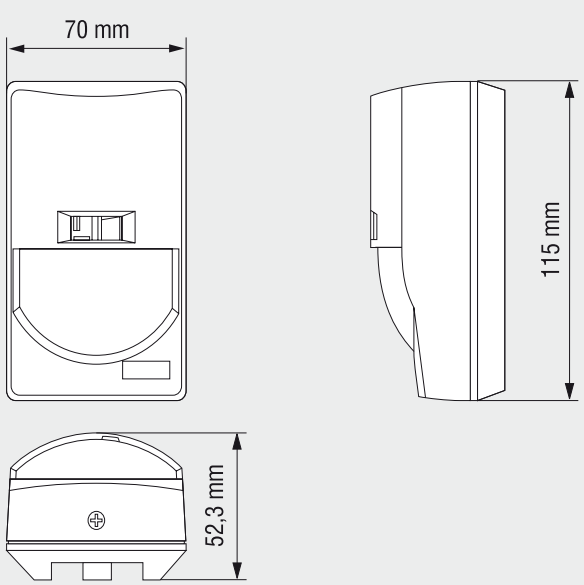
Antymasking (CX-502AM) to funkcja umożliwiająca wychwycenie prób zasłonięcia czujki i wyeliminowania jej w ten sposób z systemu alarmowego. Wykorzystanie naturalnych zjawisk emisji promieniowania podczerwonego przez wszystkie istoty żywe pozwala w stosunkowo łatwy i niedrogi sposób wykrywać obecność intruza w chronionej przestrzeni. Jednakże, ze względu na właściwości fizyczne światła, przesłonięcie pola widzenia czujki przesłoną z jakiegokolwiek materiału powoduje, że promieniowanie emitowane w obszarze obserwacji czujki do niej nie dociera. Funkcja antymaskingu ma umożliwić sygnalizację przypadkowego zasłonięcia czujki, np. w wyniku zmian konfiguracji umeblowania pomieszczenia, lub – co bardziej istotne – sygnalizować próbę celowego jej zasłonięcia (np. zaklejenia lub zamalowania soczewki) w celu całkowitego wyłączenia bądź przynajmniej zmniejszenia skuteczności detekcji. Skuteczność wykrywania prób sabotażu jest więc bardzo ważna dla czujek klasy S, ponieważ umożliwia ochronę systemu alarmowego przed aktywnością przestępców dysponujących wysokiej jakości sprzętem i wiedzą na temat technologii zabezpieczeń.

Nie powinno więc dziwić, że udoskonalenia dokonane w modelu CX-502AMplus dotyczą głównie realizacji funkcji antymaskingu. W obu modelach (CX-502AM i CX-502AMplus), funkcja antymaskingu realizowana jest przez wykorzystanie promieniowania podczerwonego. Unikatowy układ antymaskingu modelu CX-502AM składa się z dwóch elementów emitujących promieniowanie (jeden za soczewką układu optycznego, drugi w przedniej części obudowy) oraz z elementu światłoczułego (również w przedniej części obudowy). Funkcjonowanie tego układu opiera się na odbiciu promieniowania podczerwonego od ewentualnych przeszkód znajdujących się przed czujką. Osiągnięcie wystarczająco dużego poziomu promieniowana na elemencie światłoczułym powoduje aktywację wyjścia T.O. Dzięki odpowiedniemu uformowaniu pryzmatów układ jest w stanie wykrywać wszelkie próby maskowania, łącznie z przezroczystymi substancjami nanoszonymi na powierzchnię soczewki w formie sprayu. W związku z tym, że każda czujka pracuje w innych warunkach otoczenia (poziom promieniowania tła, zakres temperatur pomieszczenia itd.), czujki CX-502AM przez 30 sekund od włączenia zasilania „uczą się" pomieszczenia, w którym

Charakterystyka czujek



Wymiary



zostały zainstalowane. Na tej podstawie ustalane są progi zadziałania antymaskingu dostosowane do warunków pomieszczenia. Takie rozwiązanie jest niezwykle skuteczne i zostało docenione przez projektantów i instalatorów aplikacji wysokiego ryzyka w wielu krajach na całym świecie. Bliska współpraca z klientami pozwoliła firmie Optex zidentyfikować i wyeliminować te cechy tego rozwiązania, które były nieco kłopotliwe dla instalatorów. Efektem tych działań jest nowa wersja czujki CX-502AMplus.

Udoskonalenia czujki CX-502AMplus

Zastosowanie promiennika i receptora podczerwieni w pokrywie czujnika spowodowało, że układ optyczny, jaki tworzą wraz z pryzmatem, był rozdzielany przy otwarciu obudowy. Niestety, nie zawsze instalatorzy, montujący kilkadziesiąt czujników dziennie, zwracali uwagę na to, aby nie zamieniać pokryw pomiędzy czujkami. Rozdzielenie układu optycznego oraz układu elektronicznego, do którego został on precyzyjnie dostrojony, może powodować zaburzenia pracy antymaskingu. Praktyka pokazała, że był to najczęstszy powód występowania fałszywych aktywacji układu antymaskingu w czujkach CX-502AM. Ze względu na umieszczenie elementu światłoczułego należało uważnie projektować położenie czujek względem źródeł światła. O ile sama czujka PCP jest odporna na światło białe do poziomu 50 000 lx, o tyle układ antymaskingu już znacznie mniej! Również sposób ustalania wartości progowych, czyli uruchomienia systemu, powinien odbywać się w typowych warunkach pracy czujek. Raz ustalony poziom zadziałania nie zmieniał się wraz z dobowym czy rocznym natężeniem promieniowania tła.

Wszystkie te problemy rozwiązano przez zastosowanie zupełnie nowego rozwiązania układu optycznego (*Spherical Lens Protection*), który w całości znajduje się pod soczewką czujki. Pozwoliło to zmniejszyć liczbę komponentów i umieścić wszystkie w jednym module czujki. Wyeliminowano w ten sposób główną przyczynę ryzyka nieprawidłowej pracy – zamiana obudowy nie wpływa już na jakość pracy czujki. Rozwój algorytmów adaptacyjnych oraz miniaturyzacja procesorów dużej mocy obliczeniowej umożliwiła zmianę algorytmu decyzyjnego, który w nowym rozwiązaniu dostosowuje się do warunków otoczenia (*Digital Antimasking Technology*). Używając nowej wersji czujek (CX-502AMplus), nie trzeba dbać o to, aby system był uruchamiany w najbardziej typowych dla danej lokalizacji warunkach pracy, co pozwala na zaoszczędzenie cennego czasu instalatorów.

Podsumowanie

Produkty firmy Optex należą do światowej czołówki urządzeń ochrony mienia. Firma dokłada starań, aby dostarczyć swoim klientom produkty, które będą odpowiadały ich potrzebom. Czujki CX-502, choć są w ofercie firmy od dłuższego czasu, są nadal jednym z najlepszych w swoim segmencie produktów na rynku. Wprowadzenie na rynek nowej wersji czujki CX-502AMplus, wyprzedzającej wymagania klienta w zakresie oferowanych usprawnień, nie pozostawia wątpliwości co do rzetelności firmy jako partnera oferującego profesjonalne rozwiązania w dziedzinie ochrony mienia.

Wszystkie opisane w niniejszym artykule urządzenia są do nabycia w przedstawicielstwach firmy AAT-T, która jest autoryzowanym dystrybutorem firmy Optex w Polsce.

Jarosław Gibas
Optex Security

Moduł GSM/GPRS CS7002

W kolejnym artykule poświęconym serii Comfort przybliżę Państwu moduł CS7002 z dwukierunkową komunikacją GSM/GPRS. Jako jeden z niewielu produktów na rynku umożliwia zarówno wysyłanie komunikatów, jak i zdalne zarządzanie pracą centrali

Za pomocą modułów CS7002 i CS534 można zdalnie sterować systemem i korzystać z 2-kierunkowego powiadamiania audio. Dostępna jest także funkcja zdalnego sterowania systemem dzięki usłudze SMS. Instalatorzy mogą także zdalnie programować panel centrali, wykorzystując oprogramowanie UDx75 służące do ładowania danych i ich pobierania.

Centrale Serii Comfort mają możliwość łączenia się i przekazywania informacji na pięć sposobów, a mianowicie przez:
a) łącze modemowe,
b) łącze modemowe z funkcją PAS (pominięcie automatycznej sekretarki),
c) połączenie bezpośrednie – port szeregowy,
d) sieć TCP/IP,
e) GSM/GPRS.

Informacje podstawowe

CS7002 jest modułem GPRS, który można dodać do panelu CSX75. Funkcje modułu CS7002 są następujące:
- bezprzewodowe powiadamianie o zdarzeniach,
- powiadamianie za pośrednictwem sieci PSTN lub ISDN,
- rozwiązania zapasowe dla sieci PSTN/ISDN,
- powiadamianie SIA za pomocą protokołu TCP/IP w sieci GPRS,
- powiadamianie XSIA za pomocą protokołu TCP/IP w sieci GPRS,
- przesyłanie identyfikatora kontaktu za pomocą protokołu TCP/IP w sieci GPRS,
- powiadamianie przez SMS w systemie HomeText (jawnym tekstem),
- powiadamianie SIA opcjonalnymi modyfikatorami obszaru dzięki SMS-om,
- powiadamianie XSIA przez SMS-y,
- ładowanie/pobieranie bezprzewodowe z wykorzystaniem połączenia CSD w sieci GSM,
- opcjonalne automatyczne sesje pobierania (są one zazwyczaj zwane wywołaniami próbnymi),
- zapas dla dialerów zewnętrznych.

Moduł CS7002 umożliwia:
a) skonfigurowanie 12 docelowych miejsc wysyłania raportów,
b) wybór zdarzeń z ośmiu obszarów, o których będzie powiadamiał system,
c) wykorzystywanie nie tylko sieci PSTN, ale także sieci GSM przez panel sterowania (informacja o wszystkich protokołach obsługiwanych przez panel za pomocą sieci GSM),
d) zdalną i lokalną aktywację ładowania/pobierania danych.

Konfiguracja systemu

Moduł GPRS CS7002 działa w systemie zawierającym poniższe elementy:
- centrala z serii CSX75,
- co najmniej jedna klawiatura podłączona do magistrali rozszerzania panelu sterowania,
- moduł CS5500 w wersji 2 lub nowszej i oprogramowanie panelu obsługujące moduł CS7002.

Elementy opcjonalne:
a) moduł odsłuchu CS534 i moduł głosowy CS535,
b) dialer ISDN CS7501,
c) inne opcjonalne moduły podłączone do magistrali rozszerzania panelu sterowania.

Uwaga! Aby skonfigurować raportowanie HomeText dla wiadomości SMS, użytkownik musi dysponować telefonem komórkowym.

Raporty

Informacje podstawowe

Przy wystąpieniu zdarzenia, w zależności od sposobu zaprogramowania modułu CS7002, jest ono formatowane jako zdarzenie XSIA, SIA lub Contact ID. Możne je następnie wysłać za pomocą protokołu TCP/IP, wiadomości e-mail lub SMS. Raportowanie TCP/IP może być przeprowadzane w sieci GPRS (PPP). Raportowanie SMS może być przeprowadzane w sieci GSM.

Instalator ma do dyspozycji dwanaście miejsc docelowych raportowania. Raportowanie SMS może używać maksymalnie dwóch miejsc docelowych, raportowanie TCP/IP także maksymalnie dwóch, a raportowanie HomeText – ośmiu.

Dostępnych jest sześć konfigurowalnych kontrolerów raportowania. Każdemu kontrolerowi można przypisać główne i zapasowe miejsce docelowe.

Dostępne są trzy protokoły raportowania, a każdemu przypisana jest maksymalna liczba wystąpień.

Moduł CS7002 może wysyłać powiadomienia główne, dodatkowe i zapasowe.

HomeText

HomeText to nowy protokół raportowania, który wysyła wiadomość SMS o odnotowanych zdarzeniach pod numer telefoniczny. Raporty HomeText są podobne do raportów w dzienniku zdarzeń wyświetlanych na klawiaturze.

Raportowanie HomeText korzysta z wiadomości SMS do wysyłania raportów w wybranym języku. Może używać do sześciu miejsc docelowych raportowania.

Każde miejsce docelowe raportowania składa się z:

artykuł sponsorowany

– podstawowej opcji transportu raportu (grup raportowania HomeText 1–8, SMS 1, SMS 2 itp.), oraz
– listy zdarzeń.

Przy raportowaniu HomeText można zapisać do 16 numerów telefonów. Każdy numer może należeć do dowolnego połączenia ośmiu grup raportowania HomeText i należy przypisać mu jeden z 12 dostępnych języków. Grupa raportowania HomeText może zostać wysłana do jednego z miejsc docelowych raportowania, które raportują określone zdarzenia. Wszystkie numery telefonów należące do grupy raportowania HomeText będą odbierać wiadomości SMS zdarzeń tej grupy.

Kontrola raportowania HomeText

Raportowanie HomeText umożliwia użytkownikowi wysyłanie i odbieranie wiadomości SMS z telefonu komórkowego w celu kontroli systemu zabezpieczeń. Wiadomości mogą zawierać hasło, polecenia i wartości (system można skonfigurować do używania hasła; w takim przypadku hasło należy wprowadzać przed poleceniem, czyli instrukcjami przesyłanymi do systemu zabezpieczeń).

Metody raportowania

SMS

Raporty SMS można wysyłać w formatach SIA, XSIA oraz Contact ID. Dla każdego miejsca docelowego można skonfigurować jedną listę zdarzeń.

TCP/IP

Raporty TCP/IP można wysyłać w formatach SIA, XSIA oraz Contact ID. Dla każdego miejsca docelowego można skonfigurować jedną listę zdarzeń.

Połączenie GSM CSD (oddzwanianie dla przekazywania/pobierania danych z audio)

Połączenie GSM CSD to funkcja umożliwiająca przekazywanie/pobieranie danych bez ponoszenia dodatkowych kosztów numeru telefonu/usługi CSD. Zamiast tego można zadzwonić pod numer telefonu, aby rozpocząć sesję przekazywania/pobierania danych.

Połączenie GPRS

Połączenie jest nawiązywane w sieci TCP/IP. Zamiast numeru telefonu ustawiany jest adres IP. Pomijane są opcje *Call Back Req'd* (oddzwanianie przed połączeniem) i *Allow Calls From* (akceptuj numer telefonu).

Test automatyczny

Okresowy test automatyczny można uruchamiać w celu sprawdzenia, czy system działa prawidłowo. Panel sterowania można skonfigurować tak, aby uruchamiał testy automatyczne i umieszczał zdarzenia testu automatycznego w dzienniku zdarzeń bez raportowania o nich. Następnie można skonfigurować moduł GPRS CS7002, aby powiadamiał o zdarzeniach testu automatycznego.

Nowe rozwiązania z dwukierunkową komunikacją dają ogromne możliwości zarówno instalatorom, jak i użytkownikowi. Możliwość połączenia się z centralą zainstalowaną w obiekcie z dowolnego miejsca i oprogramowanie jej, a także sprawdzenie stanu obszarów, włączenie czy wyłączenie ich z dozoru, nie stanowi już bariery. Łatwy i szybki dostęp do informacji to przecież podstawowa zasada w dzisiejszych czasach.

Witold Bach
GE Security

Nowoczesny monitoring? Co to takiego? Nowoczesny, czyli taki, który z miesiąca na miesiąc, z roku na rok spełnia coraz większe oczekiwania klientów. Rozpowszechnienie monitoringu spowodowało rozwój technologii, w tym również bezprzewodowych

Transmisja bezprzewodowa
obrazu i dźwięku 5,8 GHz

W życiu codziennym stosowane od dawna systemy bezprzewodowe upraszczają obsługę wielu urządzeń. Zapewne wielu z nas ciężko byłoby sobie wyobrazić życie bez telefonów bezprzewodowych, zdalnego sterowania bramą garażową czy też zwykłego pilota do telewizora. I choć prościej byłoby podłączyć je kablem, wielu wybiera rozwiązania bezprzewodowe. Tak też jest z monitoringiem. Wielu z instalatorów i ich klientów wybiera systemy bezprzewodowe. Dlatego firma „3D" od kliku lat produkuje systemy bezprzewodowe. Najpierw były to systemy pracujące w paśmie 1,2 GHz, potem 2,4 GHz, a obecnie poszerzyliśmy swoją ofertę o systemy pracujące w paśmie 5,8 GHz. Kilkuletnie doświadczenie w produkcji systemów bezprzewodowych transmisji obrazu i dźwięku stawia nas na pozycji lidera w tej dziedzinie.

Charakterystyka systemu transmisyjnego 5,8 GHz – RTR05-h

Obecnie korzysta się z dwóch technologii transmisji wideo: analogowej i cyfrowej, jednak stosowane są do realizacji innych funkcji – transmisja analogowa w układach lokalnych, cyfrowa – na większe odległości. W paśmie 2,4 GHz urządzenia analogowe i cyfrowe pracują jednocześnie co zwiększa liczbę zakłóceń. Pasmo 5,8 GHz charakteryzuje się rozdziałem transmisji cyfrowych (Internet itp.) od analogowych, co zdecydowanie ogranicza liczbę zakłóceń.

Bezprzewodowy system transmisji obrazu i dźwięku 5,8 GHz (RTR05-h CAMSAT) oparty na nowoczesnej technologii i rozbudowanej obróbce sygnału wizyjnego poprawia jakość sygnału oraz eliminuje interferencje. Zestaw w wersji podstawowej (nadajnik i odbiornik w obudowie hermetycznej, zintegrowane z anteną kierunkową) uzyskuje transmisję do 2000 metrów. Zastosowanie dodatkowych anten kierunkowych (zewnętrznych) może transmisję zwiększyć nawet do 5000 metrów. Zestaw pozwala na wybór aż ośmiu kanałów pracy oraz na integrację rozbudowanych systemów. Charakter pasma 5,8 GHz nakazuje bezwzględnie przestrzegać widzialności anteny nadawczej z odbiorczą. Praca urządzeń tego typu pozbawiona jest konieczności posiadania zezwoleń, natomiast samo urządzenie posiada wiele dokumentów potwierdzających zgodność z przepisami (Zgodny z FCC – Federal Communications Commission rozdział 15.247 (ISM), Zgodny z IC – Industry Canada RSS-210, RSS-139 oraz znak CE).

Odbiornik RT05-h i nadajnik TR05-h zostały zaprojektowane jako kontynuacja i rozwinięcie idei bezprzewodowego przesyłu sygnałów audio i wideo głównie na potrzeby telewizji przemysłowej. Są to 8-kanałowe urządzenia. Użytkownik może wybrać manualnie jeden z ośmiu kanałów pracy za pomocą nastawników (5733, 5752, 5771, 5790, 5809, 5828, 5847, 5866 MHz). Posiadają one wejścia/wyjście wideo oraz dwa wejścia/wyjścia audio, pozwalają przesłać sygnał dźwiękowy stereo. Do gniazda wideo odbiornika możemy podłączyć odbiornik telewizyjny, magnetowid, rejestrator, a do gniazda wideo nadajnika – sygnał z kamery (b/w, color), tunera, magnetowidu czy innego źródła. Urządzenia zasilane są napięciem DC 12 V, 500 mA.

Pobór prądu odbiornika to 170 mA, nadajnika: 140 mA. Zestaw transmisyjny umieszczony jest w obudowie hermetycznej (IP 67), więc nadaje się do zastosowań zewnętrznych i pracuje w temperaturach od -20°C do +70°C.

System RTR05-h jest bardzo prosty w obsłudze, wystarczą podstawy wiedzy o systemach bezprzewodowych, np. o obsłudze RTR02-h CAMSAT – bezprzewodowego systemu transmisyjnego pracującego w paśmie 2,4 GHz (wykonanie hermetyczne) oraz wnikliwa lektura instrukcji.

Co dalej po systemie RTR05-h, jaki rozwój?

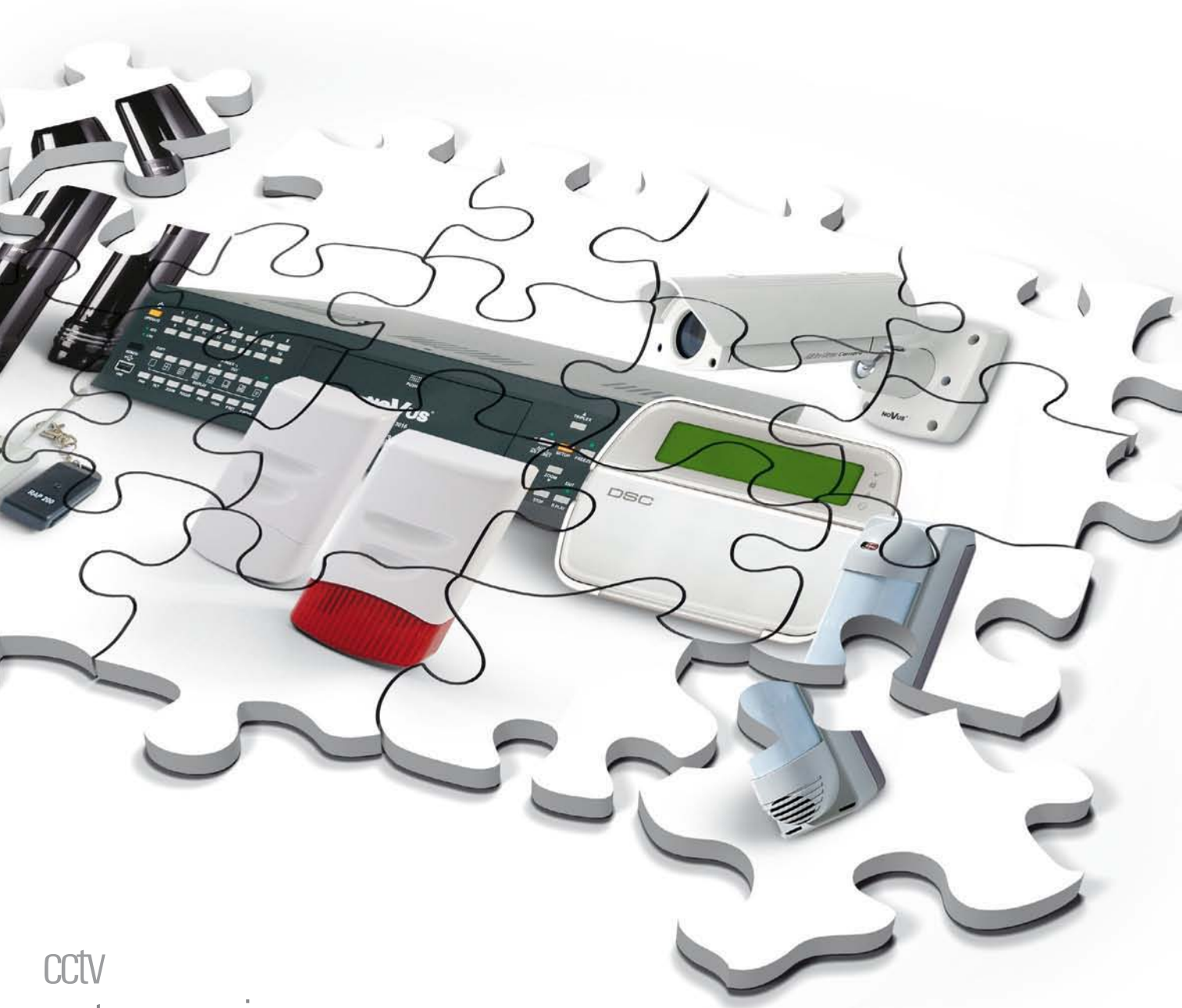
Podążając za potrzebami nowoczesnego monitoringu, firma „3D" z Bydgoszczy planuje w najbliższym czasie wprowadzić do sprzedaży bezprzewodowe moduły telemetryczne, zapewniające zdalną obsługę kamer obrotowych, stosowanych coraz częściej w monitoringu dużych obiektów. Wspomniane moduły telemetryczne pracują w dozwolonych pasmach 433 MHz; 868 MHz; 2,4 GHz; 5,8 GHz, umożliwiają transmisję danych w standardzie RS485 z wykorzystaniem protokołu np. PELCO D lub innych. Będzie to nasze własne rozwiązanie konstruktorskie, oparte na wieloletniej pozycji w branży, doświadczeniu i wysoko wykwalifikowanej grupie specjalistów.

Jowita Kuczyniecka
„3D" Bydgoszcz
www.3d.com.pl

wszechstronność

funkcjonalność

profesjonalizm



cctv

systemy ppoż

systemy SSWiN

kontrola dostępu

osprzęt i akcesoria

systemy monitoringu

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

artykuł sponsorowany

Szybki rozwój telefonii komórkowej GSM oraz rosnący zasięg pozwolił na jej wykorzystanie w systemach monitorowania zdarzeń alarmowych. Informacja z centrali alarmowej zainstalowanej w chronionym obiekcie przekazywana jest, przez sieć GSM, do centrum monitorowania. Na rynku istnieje wiele rodzajów nadajników, niestety niewiele firm podejmuje się zaprojektowania stacji odbiorczej, która stanowi integralną część systemu monitorującego. Zazwyczaj realizowana jest ona w postaci programu komputerowego, co nie daje gwarancji niezawodnego działania. Jakość jej pracy jest zależna od zastosowanego systemu operacyjnego, na którego budowę, a więc i stabilność, nie mamy wpływu. W artykule przedstawiono zasadę działania stacji odbiorczej zaprojektowanej do monitorowania systemów alarmowych z wykorzystaniem sieci GSM/GPRS. Zaproponowane rozwiązanie zapewnia niezawodną pracę urządzenia niezależnie od systemu komputerowego

Nowa stacja odbiorcza monitorowania systemów alarmowych z wykorzystaniem sieci GSM/GPRS

Wprowadzenie

SMSCI (fot. powyżej) jest urządzeniem przeznaczonym do monitorowania stanów i zdarzeń generowanych przez systemy alarmowe. Wykorzystuje infrastrukturę sieci komórkowej GSM (ang. *Global System for Mobile Communications*) do przesyłania informacji o zdarzeniach. Komunikaty przesyłane są w postaci krótkich wiadomości tekstowych SMS (ang. *Short Message Service*) lub wykorzystując pakietową transmisję danych GPRS (ang. *General Packet Radio Service*). Realizowana jest również identyfikacja zdarzeń typu CLIP (ang. *Calling Line Identification Presentation*), gdzie stała informacja (przeważnie test) jest przypisana próbie nawiązania połączenia głosowego przez nadajnik abonencki ze stacją odbiorczą.

Architektura

SMSCI zaprojektowano modułowo. Urządzenie składa się z sześciu podsystemów odbiorczych umiejscowionych na trzech kartach mocowanych w obudowie o wysokości 3U, umożliwiającej montaż w stojakach o szerokości 19”. Możliwe jest dostosowanie konfiguracji urządzenia do potrzeb centrum monitorowania wynikających z intensywności ruchu informacyjnego oraz typu zastosowanej transmisji (SMS lub GPRS). Schemat blokowy urządzenia przedstawiono na rys. 1. Podstawę SMSCI stanowią trzy karty: „KONTROLER”, „WYŚWIETLACZ I AKUMULATOR” oraz „KLAWIATURA I ZASILACZ”, które występują w każdej konfiguracji.

Karta „KONTROLER” odpowiedzialna jest za odbiór zdarzeń z torów odbiorczych i przesłanie ich do komputera lub wyświetlenie na wyświetlaczu ciekłokrystalicznym.

Interfejs komunikacyjny stanowi ośmiobitowa równoległa szyna danych, na której ruch regulowany jest z wykorzystaniem dodatkowych linii sterujących. Zaimplementowano protokół transmisji typu Nadrzędny–Podrzędny. Maksymalna szybkość transmisji, w zrealizowanym interfejsie, wielokrotnie przekracza możliwości transmisyjne torów odbiorczych, co umożliwia przesyłanie dodatkowych komunikatów systemowych, informujących o stanie pracy wszystkich podsystemów urządzenia. Karta „KONTROLER”, jako urządzenie typu Nadrzędny, odpytuje wszystkie odbiorniki, sprawdzając, czy są w nich zdarzenia oczekujące na transmisję. W czasie nieaktywności (brak komunikatów z nadajników abonenckich) przesyłane są ramki podtrzymania łączności, które pozwalają na kontrolę poprawności pracy torów odbiorczych. Dane archiwizowane są w buforze pamięci o pojemności 100 zdarzeń. W zależności od aktualnego trybu pracy komunikaty przesyłane są do programu bazy danych zainstalowanego na współpracującym z SMSCI komputerze lub do wyświetlacza. Karta „KONTROLER” posiada wbudowany zegar czasu rzeczywistego, ustawiany z klawiatury urządzenia. Dostarcza on informacji pozwalającej na nadanie stempla czasowego odbieranym zdarzeniom.

Karta „WYŚWIETLACZ I AKUMULATOR” zapewnia rozpływ prądu do wszystkich elementów urządzenia. Napięcie

z zasilacza podłączonego do sieci energetycznej stanowi główne źródło zasilana. Zabezpieczeniem awaryjnym jest wbudowany akumulator, stale kontrolowany i doładowywany z zasilania zewnętrznego. Kartę wyposażono w wyświetlacz ciekłokrystaliczny sterowany z lokalnego procesora, który jest odpowiedzialny za obsługę klawiatury i komunikację z kartą „KONTROLER".

Karta „KLAWIATURA I ZASILACZ", oprócz klawiatury, wyposażona jest w zasilacz impulsowy przymocowany do ściany bocznej obudowy, która stanowi jego radiator. Dopuszczalne napięcie wejściowe zawiera się w zakresie od 84 V do 264 V_{AC}. Układ zabezpieczony jest bezpiecznikiem 2 A (w gnieździe zasilającym). Urządzenie posiada dodatkowo wbudowany, przeciwzakłóceniowy filtr sieciowy.

Karty odbiorcze

SMSCI zostało wyposażone w maksymalnie sześć podsystemów odbiorczych, zlokalizowanych na trzech kartach. Są to: cztery tory GSM, tor SMSC oraz tor GPRS. Dwa ostatnie zlokalizowane są na pierwszej karcie urządzenia, natomiast pozostałe na karcie drugiej i trzeciej, licząc od lewej strony (zob.: zdjęcie na poprzedniej stronie).

Podsystem GSM

Podsystem GSM jest odpowiedzialny za odbiór drogą radiową sygnałów w postaci wiadomości SMS i CLIP z nadajników abonenckich. Sygnał z anteny GSM przesyłany jest do złącza na tylnym panelu obudowy. W skład podsystemu wchodzą: przemysłowy moduł GSM i sterownik, odpowiedzialny za inicjalizację i kontrolę poprawności działania toru oraz łączność z kontrolerem. Struktura urządzenia pozwala na jego samodzielną i niezależną od reszty układu pracę. Dzięki temu wszelkie problemy w jego funkcjonowaniu, wynikające z zakłóceń w pracy sieci GSM, mogą być rozwiązywane lokalnie, nie wpływając na pozostałe elementy systemu (odbior zdarzeń od pozostałych podsystemów nie jest opóźniony). Można stosować różnego typu przemysłowe moduły GSM.

Sterownik odpowiedzialny jest za poprawne logowanie modułu do macierzystej sieci komórkowej. W trakcie pracy kontrolowana jest moc sygnału GSM, której stan jest sygnalizowany zieloną lampką na panelu czołowym karty. Krótkie mignięcia, co 0,5 sekundy, których liczba odpowiada poziomowi mocy sygnału odbieranego w module GSM, rozdzielone są pojedynczym długim wyłączeniem (na 2 sekundy). Pomiar mocy sygnału realizowany jest w module GSM. Obniżenie jego poziomu poniżej ustalonego progu, trzykrotnie stwierdzone przez sterownik, wyzwala procedurę restartu modułu GSM. Stan mocy odbieranego sygnału GSM dołączany jest do każdej depeszy przesyłanej do komputera (zob. więcej na ten temat w dalszej w części artykułu). Podczas braku ruchu informacyjnego (SMS lub CLIP) generowany jest komunikat podtrzymania łączności z kontrolerem, w którym również przesyłana jest informacja o aktualnej mocy sygnału.

Podsystem SMSC

Podsystem SMSC jest odpowiedzialny za komunikację z SMSC (ang. *Short Message Service Center*) operatora sieci telefonii komórkowej za pomocą łącza w standardzie Ethernet, z zastosowaniem protokołów komunikacyjnych TCP/IP (ang. *Transmission Control Protocol*/*Internet Protocol*). Umiejscowione na tyle obudowy gniazdo RJ45, umożliwia podłączenie do sieci LAN (ang. *Local Area Network*). Połączenie z serwerem SMSC, w zależności od dostępnej infrastruktury, może być zrealizowane przez publiczną sieć Internet, łącze dzierżawione stałe lub radiolinię. W podsystemie SMSC zaimplementowano, odpowiednie dla każdej sieci komórkowej GSM, protokoły komunikacyjne. Realizują one połączenie z warstwą aplikacji SMSC, zapewniając formatowanie oraz kontrolę dostarczenia informacji (protokół z potwierdzeniami). Zgodnie ze standardem protokołu podsystem SMSC odbiera zdarzenia SMS bezpośrednio z serwera SMSC, omijając konieczność nawiązania połączenia i transmisji komunikatów drogą radiową, co znacznie skraca czas dostarczenia informacji. Zaimplementowane protokoły komunikacyjne pozwalają na wymianę informacji z większością pracujących w Polsce serwerów SMSC. Stan pracy podsystemu SMSC sygnalizowany jest na panelu czołowym (stan aktywny – kolor zielony, brak połączenia – kolor czerwony).

Podsystem GPRS

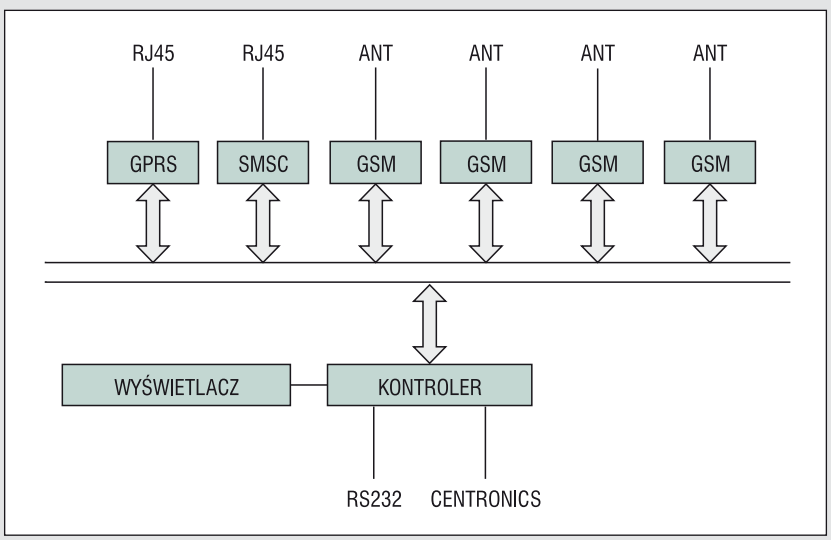
Podsystem GPRS jest odpowiedzialny za odbiór i interpretację sygnałów wysyłanych z nadajników abonenckich z wykorzystaniem pakietowej transmisji danych GPRS. Komunikacja odbywa się za pomocą łącza w standardzie Ethernet z zastosowaniem protokołu UDP (ang. *User Datagram Protocol*) przez prywatny lub publiczny APN (ang. *Access Point Name*) operatora telefonii komórkowej. W torze GPRS, podobnie jak w torze GSM, abonent identyfikowany jest przez numer telefonu karty SIM zainstalowanej w nadajniku. Dzięki takiemu rozwiązaniu, zdarzenia, niezależnie od sposobu transmisji, są jednoznacznie identyfikowane w stacji odbiorczej. Pozwala to również na stosowanie w nadajnikach abonenckich kart SIM z dynamicznie przydzielanym, niepublicznym adresem IP. Nie ma konieczności aktywowania dodatkowych, odpłatnych, usług dla tych kart, takich jak stały adres IP lub grupowanie numerów w ramach prywatnego APN. Zastosowanie publicznego APN upraszcza również konfigurację systemu po stronie stacji odbiorczej. Konieczne jest jedynie zapewnienie połączenia z Internetem, ze stałym i publicznym adresem IP. W celu zwiększenia bezpieczeństwa należy stosować zaporę sieciową (ang. *Firewall*) blokującą niepowołany dostęp do stacji odbiorczej z zewnątrz. Powinna ona zapewniać dostępność portu, przez który nadajniki abonenckie komunikują się z podsystemem GPRS, od strony sieci publicznej.

Na potrzeby łączności nadajnika abonenckiego ze stacją odbiorczą zrealizowano protokół komunikacyjny z potwierdzeniami, który zapewnia kontrolę poprawności transmisji danych. Zdarzenia alarmowe odbierane przez podsystem GPRS automatycznie przesyłane są do programu bazy danych zainstalowanego w centrum monitorowania. W odróżnieniu od transmisji SMS zastosowano dwa rodzaje komunikatów testowych: testy jawne, traktowane jak zdarzenia alarmowe (przesyłane do programu bazy danych) oraz testy niejawne (TN), analizowane i przetwarzane w podsystemie GPRS. Zadaniem TN jest kontrola poprawnej pracy i łączności nadajnika abonenckiego ze stacją odbiorczą. Brak testu w czasie trzech kolejnych okresów sygnalizowany jest zdarzeniem alarmowym oznaczającym utratę łączności z nadajnikiem abonenckim. Opóźnienie pomiędzy uszkodzeniem abonenckiego sytemu alarmowego (brak łączności) i jego sygnalizacją w centrum monitorowania jest zależne od częstotliwości nadawania TN. Zgodnie z normą PN-EN50136-1-1:2002 (PN-93/E-08390/51) zaimplementowano obsługę kontroli dostarczenia TN dla trzech interwałów czasowych (stosownie do odpowiednich klas bezpieczeństwa): T3 (65 minut), T4 (90 sekund), T5 (20 sekund). W podsystemie GPRS utworzono trzy bazy danych, w których rejestrowane są nadajniki abonenckie. Zostały one skojarzone z czasookresami TN, dla

których przydzielono niezależne obszary pamięci. Zarejestrowanie nowego numeru następuje po odbiorze pierwszego TN. Zdarzenie to sygnalizowane jest komunikatem „NN". Przekroczenie kolejnych dziesięcioprocentowych progów wypełnienia każdej z baz sygnalizowane jest komunikatami alarmowymi (np. przekroczenie 10% zajętości bazy dla testów klasy T4 generuje komunikat „21" z numerem abonenta „000000000"). Podsystem GPRS analizuje liczbę nadajników abonenckich, z którymi nastąpiła utrata łączności w czasie pojedynczego okresu testu. Przekroczenie ustalonego progu powoduje wstrzymanie transmisji zdarzeń sygnalizujących utratę łączności oraz wygenerowanie komunikatu informacyjnego. Funkcja ta ma na celu niedopuszczenie do przesłania w krótkim czasie dużej liczby zdarzeń informujących o utracie łączności spowodowanej awarią lub wyłączeniem usługi GPRS na obszarze, na którym zainstalowano nadajniki abonenckie. Baza danych nadajników abonenckich jest automatycznie, co 24 godziny, archiwizowana w nieulotnej pamięci Flash. Procedura ta może zostać wymuszona ręcznie przez wciśniecie przycisku na panelu czołowym karty, dzięki czemu nie ma obawy, że dane zostaną utracone podczas prac konserwacyjnych.

W podsystemie GPRS zastosowano 32-bitowy procesor wykonany w technologii ARM (ang. *Advanced RISC Machine*) firmy NetSilicon. Układ pracuje z zegarem 55 MHz. Architektura Harvard, z rozdzielonymi pamięciami danych i programu oraz technologią RISC (ang. *Reduced Instruction Set Computers*), gdzie rozkazy wykonywane są w ściśle określonym czasie, przeważnie w jednym cyklu maszynowym, zapewnia dużą wydajność pracy. Procesor wraz z układami zewnętrznymi stanowi specjalizowany system do zastosowań sieciowych.

Rys. 1. Schemat blokowy SMSCI



Zdarzenia

Zdarzenia alarmowe odbierane przez SMSCI zawierają informację o numerze abonenta (numer telefonu karty SIM zainstalowanej w nadajniku) oraz szczegółowe dane opisujące zdarzenie. Komunikaty można podzielić na:

– zdarzenia dwuznakowe: informacja o typie alarmu kodowana jest dwoma znakami, które mogą być grupowane do czterech zdarzeń w jednej ramce;
– zdarzenia typu Contact-ID: przesyłana jest informacja o kodzie zdarzenia, numerze partycji i strefy;
– zdarzenia trzynastoznakowe w formacie Dyskam.

Przyjmując jako kryterium podziału sposób transmisji, wyróżniamy zdarzenia typu SMS/GPRS lub CLIP.

Zdarzenia SMS/GPRS

Zarówno w zdarzeniach SMS, jak i GPRS informacja o alarmie przesyłana jest w postaci pakietu danych. Dla obu typów wiadomości numer telefonu przypisany do karty SIM stanowi kod identyfikujący abonenta. Dzięki temu wszystkie komunikaty docierające do stacji odbiorczej z tego samego nadajnika, niezależnie od trybu pracy (SMS czy GPRS), są jednoznacznie identyfikowane. Aby zapewnić powyższą sygnalizację w zdarzeniach typu GPRS, nadajnik musi mieć informację o numerze telefonu. W nadajnikach abonenckich firmy PULSON informacja ta zapisana jest w pamięci karty SIM pod pozycją „NUMER WŁASNY". Większość kart SIM aktywowanych przez operatora ma zapisany „NUMER WŁASNY", zdarza się jednak, że nie został on zapisany. W takim wypadku można go zaprogramować, wykorzystując funkcję automatycznego programowania numeru telefonu w nadajniku abonenckim zrealizowaną w podsystemie GSM urządzenia. Nadajnik abonencki wysyła wiadomość z zapytaniem o własny numer telefonu do modułu GSM zainstalowanego w SMSCI, który odsyła żądaną informację. Stacja odbiorcza dodatkowo generuje odpowiedni komunikat systemowy informujący o przeprowadzonym działaniu. Zdarzenia typu SMS wzbogacone są dodatkowo, przez system GSM, o informację o czasie nadania wiadomości, która przesyłana jest do programu bazy danych zainstalowanego w centrum monitorowania.

Zdarzenia CLIP

Zdarzenia typu CLIP generowane są podczas próby nawiązania przez nadajnik abonencki połączenia głosowego z modułem GSM zainstalowanym w SMSCI. Podsystem GSM, wraz z sygnałem dzwonienia, otrzymuje informację o numerze telefonu dzwoniącego. Taka sygnalizacja zdarzeń alarmowych lub testowych jest możliwa pod warunkiem, że identyfikacja numeru dzwoniącego została uaktywniona przez operatora telefonii komórkowej dla karty SIM zainstalowanej w odbiorniku. SMSCI automatycznie odrzuca próbę nawiązania połączenia rozmownego, co redukuje do minimum zajętość kanału sygnalizacyjnego. Zdarza się, że sygnał identyfikacji dzwonienia w odbiorczym module GSM jest generowany, zanim infrastruktura sieci GSM zostanie przygotowana do zestawienia połączenia głosowego (badania własne). W tym momencie odrzucenie próby nawiązania połączenia rozmownego przez moduł odbiorczy powoduje zaburzenie pracy sieci komórkowej. Może ono doprowadzić do konieczności restartu nadawczego i odbiorczego modułu GSM. W podsystemie GSM stacji odbiorczej zrealizowano opóźnienie rozłączenia, którego czas zoptymalizowano tak, aby przy minimalnej zajętości kanału uzyskać minimalne prawdopodobieństwo wystąpienia opisanego problemu. Odrzucenie próby dzwonienia zrealizowano tak, aby w nadajniku abonenckim zostało ono zasygnalizowane

komunikatem „NO CARRIER”. Dzięki temu w nadajnikach abonenckich firmy PULSON możliwe było zapewnienie weryfikacji dostarczenia zdarzenia typu CLIP. Takie rozwiązanie zwiększa wiarygodność systemu monitorowania. Sprawność systemu odbiorczego istotnie wzrasta po rozdzieleniu numerów odbiorczych dla zdarzeń typu SMS i CLIP. Jest to możliwe do zrealizowania, nawet przy istniejącej infrastrukturze nadajników abonenckich, przez ustawienie, dla karty odbiorczej SIM, przekierowania wszystkich połączeń głosowych na inny numer karty SIM. Operacja ta jest bezpłatna.

Komunikacja z komputerem

SMSCI połączone jest z komputerem za pomocą interfejsu komunikacyjnego w standardzie RS232 (transmisja szeregowa ze sprzętową kontrolą przepływu danych). Zastosowano protokół komunikacyjny z potwierdzeniami, w którym informacja przesyłana jest w pakietach ze stałym formatem ramki. Oprócz znaków początku i końca przesyłane są dane o numerze abonenta, kodzie zdarzenia oraz dacie i czasie jego wystąpienia. Dodatkowo dołączona jest informacja o numerze toru odbiorczego, w którym zdarzenie zostało odebrane, oraz, w przypadku toru GSM, o tym, jaka była moc sygnału GSM w odbiorniku. Są to niezbędne informacje potrzebne do identyfikacji typu i pochodzenia zdarzenia oraz określenia sposobu jego transmisji (GSM/GPRS) i czasu dostarczenia (ewentualnie nadania). Pozwala to na ocenę intensywności ruchu komunikacyjnego w poszczególnych torach odbiorczych urządzenia oraz kontrolę jakości serwisu GSM w miejscu, w którym zlokalizowane jest centrum monitorowania.

Tryb pracy ZDALNY/LOKALNY

SMSCI pracuje w jednym z dwóch trybów: „ZDALNY”, w którym zdarzenia przesyłane są do komputera, lub „LOKALNY”, gdzie komunikaty wyświetlane są na wyświetlaczu, natomiast ich odbiór potwierdzany jest ręcznie przez operatora centrum monitorowania. Urządzenie okresowo sprawdza poprawność połączenia sprzętowego z komputerem oraz łączność z programem bazy danych (komunikacja z potwierdzeniami). Spełnienie obydwu warunków poprawnej łączności powoduje automatyczne przełączenie urządzenia w tryb pracy „ZDALNY”. Stan połączenia jest stale kontrolowany. Utrata łączności powoduje automatyczne przełączenie w tryb pracy „LOKALNY”. Każda zmiana trybu pracy urządzenia jest sygnalizowana komunikatem systemowym. Zdarzenia mogą być archiwizowane na papierze za pomocą drukarki.

Interfejs użytkownika

Interfejs użytkownika stanowi wyświetlacz ciekłokrystaliczny (2 linie po 20 znaków), klawiatura oraz zestaw sygnalizatorów świetlnych i dźwiękowych. Na wyświetlaczu, niezależnie od trybu pracy, wyświetlane są wszystkie zdarzenia. Prezentowany jest numer abonenta, kod zdarzenia (dla Contact-ID również szczegółowa informacja o warunkach jego wystąpienia) oraz informacje o czasie nadania i odbioru zdarzenia. Dodatkowo wyświetlana jest informacja o stanie zajętości buforów: komputera i drukarki, oraz aktualnym trybie pracy. Dwunastoznakowa klawiatura pozwala na programowanie parametrów pracy urządzenia:

– F-1: programowanie daty i czasu,
– F-2: załączenie lub wyłączenie druku zdarzeń w trybie „ZDALNY”,
– F-3: załączenie lub wyłączenie sygnalizacji grupy zdarzeń systemowych,
– F-4: załączenie lub wyłączenie sygnalizacji wszystkich zdarzeń systemowych,

Odpowiednie sygnalizatory świetlne na panelu czołowym każdej z kart odbiorczych wskazują stan pracy i aktywność komunikacji. Na karcie „KLAWIATURA I ZASILACZ” sygnalizowany jest stan zasilania (bateryjne/zewnętrzne), tryb pracy („ZDALNY/LOKALNY”) i stan połączenia z drukarką i komputerem.

Podsumowanie

Stacja odbiorcza jest istotnym składnikiem systemu monitorowania. Od poprawności i niezawodności jej pracy zależy bezpieczeństwo nadzorowanych obiektów. Zaproponowane rozwiązanie, dzięki zastosowaniu nowoczesnych technologii oraz oryginalnych rozwiązań funkcjonalnych, stanowi profesjonalne urządzenie zapewniające stabilną pracę w systemach monitorowania z wykorzystaniem sieci GSM. SMSCI zostało opracowane z zachowaniem zaleceń polskich norm dla systemów alarmowych i systemów transmisji alarmu. Urządzenie, w całości zaprojektowane i wyprodukowane w firmie PULSON, stanowi unikatowe rozwiązanie sprzętowe stacji odbiorczej sygnałów alarmowych przesyłanych z wykorzystaniem sieci GSM/GPRS.

Dariusz Janusek
Rafał Miklaszewski
PULSON

Idealne rozwiązanie
dla instytucji rządowych,
wojska oraz firm ceniących
sobie bezpieczeństwo

Drukarka Tango+L

Brytyjska firma Ultra Electronics Card Systems – producent drukarek MAGICARD – oferuje duży wybór wyspecjalizowanych drukarek do identyfikatorów. Najnowszym, a zarazem najbardziej zaawansowanym pod względem zabezpieczeń modelem jest drukarka Tango+L. Oferuje ona kilka stopni zabezpieczeń drukowanych kart.

Opisując właściwości wyżej wspomnianej drukarki, należy rozpocząć od jej budowy. Konstrukcja urządzenia wykonana jest z wysokiej jakości metalu, dzięki czemu jest bardzo trwała, a wygląd drukarki utrzymany jest w nowoczesnej stylistyce. Drukarka jest wyposażona w panel z przyciskami funkcyjnymi, diodami LED oraz z wyświetlaczem LCD. Na ciekłokrystalicznym wyświetlaczu prezentowane są informacje na temat aktualnego stanu urządzenia oraz operacji na nim wykonywanych. Podajnik i odbiornik kart oraz część laminacyjna drukarki są zabezpieczone przed nieautoryzowanym użyciem dwoma oddzielnymi zamknięciami na klucze.

Drukarka MAGICARD Tango+L ma wbudowany mechanizm obracający kartę, dzięki któremu w jednym cyklu możliwe jest zadrukowanie oraz zalaminowanie obu stron karty. Tango+L może również pełnić funkcję samodzielnego laminatora do kart. W takim przypadku nie jest konieczne podłączanie drukarki do komputera, a wszystkie ustawienia laminatora oraz laminacja są dokonywane za pomocą przycisków na panelu drukarki.

W zależności od potrzeb użytkownika drukarka umożliwia zastosowanie kilku rodzajów zabezpieczeń karty przed kopiowaniem. Najprostszym zabezpieczeniem jest znak wodny HoloKote umieszczany na warstwie overcoat (zabezpieczającej przed utratą kolorów i ścieraniem), który jest nanoszony w końcowej fazie nadruku karty, zaraz po naniesieniu wszystkich kolorów. W tym właśnie momencie głowica drukarki „wymraża" szablon znaku zabezpieczającego. Funkcja ta nie wydłuża czasu ani nie zwiększa kosztów wydruków. Cały proces zabezpieczenia i wydruku może odbywać się na kartach identyfikacyjnych, zbliżeniowych, stykowych i kartach samoprzylepnych PVC przeznaczonych do drukarek termosublimacyjnych.

Funkcję HoloKote można włączać i wyłączać w sterowniku drukarki.

Kolejnym stopniem zabezpieczenia jest HoloPatch – złote okno w rogu karty, w którym tekst znaku wodnego jest bezpośrednio widoczny i daje efekt podobny do hologramu (opcja dostępna przy zastosowaniu karty HoloPatch we wszystkich drukarkach Magicard).

artykuł sponsorowany

Drukarka Tango+L posiada wbudowane dwa standardowe wzory znaku wodnego. Aby podnieść stopień zabezpieczenia kart, możliwe jest umieszczenie dowolnego tekstu lub grafiki (np. logo firmy) w znaku wodnym. W takim przypadku należy zamówić dodatkowo specjalną kartę zabezpieczającą Custom Text&LOGO. Karta taka może również spełniać funkcję klucza zabezpieczającego przed nieautoryzowanym użyciem drukarki (opcja dostępna w drukarkach MAGICARD Rio 2e, Tango 2e oraz Tango+L). Po usunięciu karty Custom Text&LOGO drukarka jest zablokowana i korzystanie z niej jest niemożliwe.

W celu uzyskania bardzo trwałego nadruku lub dodatkowego zabezpieczenia przed kopiowaniem kart można wykorzystać laminator. Nakłada on na zadrukowaną kartę PVC laminat poliestrowy. Nałożenie laminatu przedłuża trwałość nadruku na karcie do około 10 000 przeciągnięć przez czytnik magnetyczny oraz przedłuża żywotność identyfikatora na wiele lat. Kolejnym zabezpieczeniem jest warstwa laminatu nałożona na znak wodny HoloKote. W takim przypadku znak wodny można zweryfikować przy użyciu światła ultrafioletowego. Można zastosować folię laminacyjną z hologramem – poza zabezpieczeniem przed uszkodzeniami mechanicznymi nadruku dodatkowo zabezpiecza ona karty przed kopiowaniem. Możliwe jest zastosowanie folii z hologramem standardowym lub spersonalizowanym (dowolna grafika). Zastosowanie spersonalizowanego hologramu wraz z własnym wzorem znaku wodnego jest najwyższym stopniem zabezpieczenia karty.

Drukarka MAGICARD Tango+L jako jedna z niewielu na świecie spełnia wymagania dyrektywy Homeland Security Presidential Directive 12 (HSPD 12), która została podpisana przez prezydenta USA w sierpniu 2004 roku jako nowy, wyższy standard zabezpieczania kart dla pracowników federalnych oraz odwiedzających ich gości. HSPD 12 dotyczy m.in. wizualnego zabezpieczenia karty, co pomaga dodatkowo w weryfikacji personelu, który ma dostęp do wydzielonych stref. Dzięki temu drukarka Tango+L wydaje się idealnym rozwiązaniem dla instytucji rządowych, wojska oraz firm ceniących sobie bezpieczeństwo na najwyższym poziomie.

Tango+L może być wyposażona w kodery do kart magnetycznych, chipowych i zbliżeniowych. Rodzaj kodera zależy od potrzeb i wymagań użytkownika. Drukarka z koderem może zakodować kartę w jednym cyklu wraz z drukiem i laminacją.

Drukarka MAGICARD Tango+L w standardzie wyposażona jest w porty: LTP, USB oraz Ethernet. Posiada sterowniki Plug&Play dla Windows (2000, XP, 2003 Server user mode oraz Vista). Obsługa drukarki (wydruk kart, wymiana materiałów eksploatacyjnych oraz konserwacja) jest bardzo prosta.

Drukarka wraz z głowicą objęta jest nielimitowaną 24-miesięczną gwarancją Ultra Cover Plus, z możliwością przedłużenia do trzech, czterech lat. Istnieje możliwość nieodpłatnego uzyskania zastępczej drukarki na czas ewentualnej naprawy.

Reasumując

MAGICARD Tango+L jest profesjonalną drukarką zaprojektowaną do wydruku dużej liczby kart, z możliwością zabezpieczenia karty zarówno przed kopiowaniem, jak i uszkodzeniami mechanicznymi, a o jej klasie może świadczyć fakt, że jest wykorzystywana między innymi do drukowania praw jazdy w Meksyku.

Acss

Tango+L – drukarka i laminator w jednym

MAGICARD

Tango+L jest termosublimacyjną drukarką kart identyfikacyjnych ze zintegrowaną stacją laminującą. Wykonana z metalowych elementów konstrukcyjnych gwarantuje wysoką niezawodność w długim okresie użytkowania. Wysoka funkcjonalność oraz zabezpieczenia drukarki i nadruku sprawiają, że jest ona profesjonalnym rozwiązaniem do masowej produkcji kart ID

Proces laminacji, podczas którego karta pokrywana jest folią poliestrową znacznie zwiększa odporność nadruku na ścieranie lub inne uszkodzenia mechaniczne. Zastosowanie folii laminacyjnych z hologramem zabezpiecza karty przed podrobieniem. Możliwe jest zastosowanie folii z hologramem użytkownika (dowolna grafika).

Tempo+L wyposażona jest w panel z przyciskami funkcyjnymi, diodami LED oraz wyświetlaczem LCD informującym o statusie drukarki.

W standardzie:

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

Stacja laminująca

2 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.

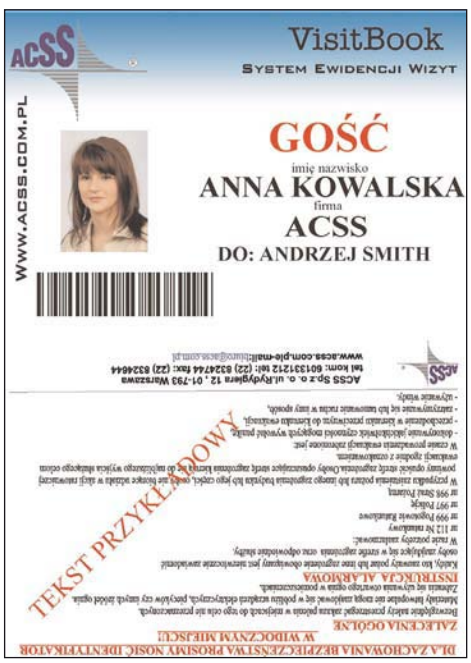
SPECYFIKACJA TECHNICZNA
PRĘDKOŚĆ NADRUKU
Nadruk z laminacją od 36 do 55 s (w zależności od ustawień)
Nadruk dwustronny z laminacją od 82 do 120 s (w zależności od ustawień)
ZABEZPIECZENIA URZĄDZENIA
Dostęp do folii laminacyjnej, podajnika oraz odbiornika kart chroniony kluczem
Zabezpieczenie przed nieautoryzowanym użyciem drukarki opcjonalną kartą flash
ZABEZPIECZENIA KART
HoloKote – znak wodny drukowany na całej powierzchni karty
Laminator (możliwość użycia folii holograficznych)
TYPY TAŚM
LC1: YMCKO – 350 wydruków
LC3: monochromatyczna – 1000 wydruków
LC6: KO (czarny i overlay) – 600 wydruków
LC8: YMCKOK – 300 wydruków
Taśmy laminacyjne czyste i holograficzne (dostępne hologramy z wzorem klienta)
Akceptowane karty
PVC/PET ISO CR80 – z paskiem magnetycznym, zbliżeniowe, HoloPatch, samoprzylepne (bez laminacji)
Grubość kart
Z laminacją – 0,76 mm
Bez laminacji – od 0,38 mm do 1.6 mm
Pojemność magazynków
Podajnik 100 szt.
Pojemnik kart nadrukowanych 50 szt.
Głowica
300 dpi
Interfejs
Port LPT i USB, Ethernet
Sterowniki
Win 2000, 2003 Server user-mode, XP
Zasilanie
240 V/50-60 Hz
Wymiary (szer. x wys. x dł.)
300 mm x 260 mm x 700 mm
Masa
20 kg
Temperatura pracy
od 10°C do 30°C

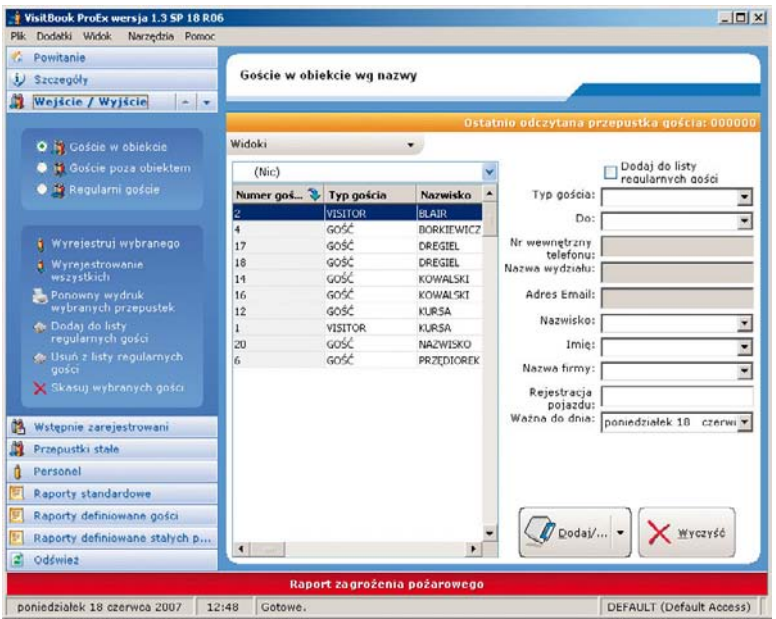
DYSTRYBUTOR w Polsce:

ACSS Sp. z o.o.
ul. Rydygiera 12, 01-793 Warszawa
tel.: 022 8324744
faks 022 8324644
e-mail:biuro@acss.com.pl
www.acss.com.pl
www.magicard.com.pl

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.

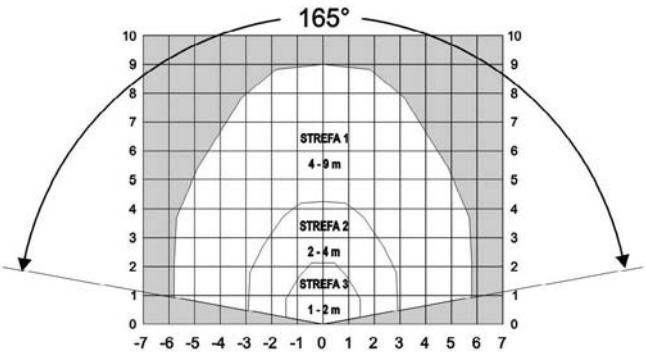
Wybrane funkcje systemu VisitBook	wersja LITE	wersja PRO	wersja PRO EX
Kontrola gości, Kontrahentów, Personelu	tak	tak	tak
Rejestracja wstępna	–	tak	tak
Lista regularnych gości	–	tak	tak
Pobieranie zdjęcia	–	–	tak
Czytnik kodów kreskowych	–	tak	tak
Elektroniczny podpis	–	–	tak
Przepustka pojazdu	–	–	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 Sp. z o.o.
ul. Rydygiera 12
01-793 Warszawa

tel. 022 832 47 44,faks 022 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl

Akustyczne detektory zbicia szyby klasy S z serii AD 700

Zakresy detekcji przy montażu na ścianie w metrach:



Produkowane przez Alarmtech detektory z serii AD 700 są nowoczesnymi, akustycznymi detektorami zbicia szyby, dającymi informację w postaci alarmu przy próbach włamania do chronionych obiektów przez okna, przeszklone drzwi, oszklone elementy ścian. Zbudowane są w oparciu o najnowszą technologię z dziedziny mikrokontrolerów, ich oprogramowanie uwzględnia wiele czynników związanych z akustyką pomieszczeń. Opracowany przez Alarmtech algorytm detekcji metodą „data fission – data fusion" uwzględnia najnowsze osiągnięcia z dziedziny techniki rozpoznawania dźwięków. Umożliwia również cyfrową kompensację akustyki pomieszczenia (DRC). Dzięki temu możliwe jest precyzyjne rozróżnianie sygnałów, powstających w wyniku zbicia szyby od innych, zakłócających.

Przeznaczone są do stosowania wewnątrz pomieszczeń – mogą być montowane na ścianach (najlepiej przeciwległych do chronionych powierzchni tak, aby okna znajdowały się w „polu widzenia" mikrofonu – 165°) i na sufitach. Instalacja na suficie nie wymaga dodatkowych akcesoriów, kształt detektora zapewnia swobodę montażu. Przy maksymalnej odległości detektora od chronionej powierzchni – 9 m, zabezpieczają szyby o grubości do 6,5 mm i wymiarach od 30 x 30 cm do 600 x 600 cm.

Kryteria dające AD 700 pozycję jednego z najbardziej interesujących akustycznych detektorów zbicia szyby:

- **Wysokiej klasy detekcja sygnału**

Dzięki algorytmowi DRC zapewniona jest znakomita detekcja sygnału rozbijanego szkła.

- **Doskonała odporność na fałszywe alarmy**

Ponownie algorytm DRC odgrywa tutaj ważną rolę razem z zaawansowanymi algorytmami rozpoznawania fałszywych alarmów.

- **Uniwersalność**

Jeden detektor może chronić wiele płaszczyzn szklanych znajdujących się w obszarze detekcji.

- **Wszechstronność**

Detektor wykrywa zbicia szkła różnego rodzaju.

- **Ulepszony sposób instalacji**

Mocowanie bez potrzeby wyjmowania płytki drukowanej. Dobry dostęp do złącz z zabezpieczeniami dla końcówek podłączanych przewodów. Łatwość programowania za pomocą przełączników – DIP.

UWAGA

Wprowadzone ostatnio do sprzedaży detektory **AD 700 S** i **AD 700 SAM** są ekonomicznymi odmianami serii AD 700, w których zrezygnowano z funkcji D/N oraz AIS przy zachowaniu wszystkich pozostałych parametrów charakterystycznych dla pełnej wersji AD 700 i decydujących o zaletach detektora.

Atesty Techom: 130/06, 131/06

Obszary zastosowań detektorów z serii AD 700		
Konstrukcja szyby		**Rodzaj szkła w szybie wewnątrz pomieszczenia**
1.	Szyby pojedyncze	Zwykłe Hartowane Laminowane
2.	Szyby podwójne zaspolone	Zwykłe Hartowane Laminowane
3.	Szyby potrójne zaspolone	Zwykłe Hartowane Laminowane
4.	Szyby pojedyncze i zespolone z folią antywłamaniową	Zwykłe z folią naklejoną od strony pomieszczenia

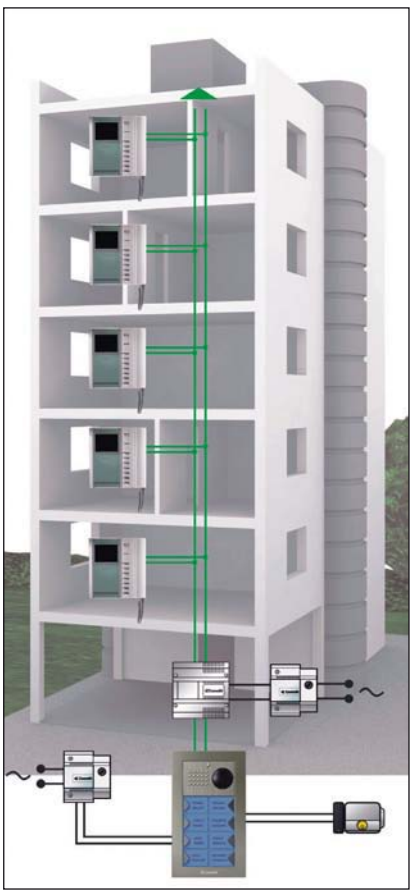
Dane techniczne	
Napięcie zasilania	9–15 V DC
Kontrola napięcia	alarm przy <7 V+/-0,5 V
Pobór prądu przy 12 V	
• w stanie spoczynkowym	ok. 25 mA
• w stanie alarmu	ok. 24 mA
Przekaźnik alarmu NC	500 mA/maks. 100 V DC R<40 ohm
Obciążalność styków przełącznika sabotażowego	50 mA/maks. 50 V DC
Zakresy	
• zasięg (maks.)	promień 9 m/165°
• zakres działania	strefa 3 = 1–2 m
	strefa 2 = 2–4 m
	strefa 1= 4–9 m
Wymiary chronionej szyby	min. 30x30 cm, maks. 6x6 m
Grubość szyby (maks.)	6,5 mm
Rodzaje szkła	zwykłe (float) – hartowane – laminowane – zwykłe foliowane
Kubatura chronionego pomieszczenia	min. 20 m^3, maks. 250 m^3
Zakres temperatury pracy	-10 do +55°C
Wilgotność, DIN 40040	maks. 90% r.h. (klasa F)
Kategoria ochr. obud. EN60529	IP 31

ALARMTECH POLSKA Sp. z o.o.

Alarmtech Polska Sp. z o.o.
80-299 Gdańsk – Osowa, ul. Kielnieńska 115
tel. 058 340-24-40, faks 058 340-24-49
http://www.alarmtech.pl; e-mail: info@alarmtech.pl

2-przewodowy system wideodomofonowy

firmy COMELIT



SIMPLEBUS2

Cechy charakterystyczne:

- 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 podczerwieni. Ramki zewnętrzne paneli dostępne są w różnych kolorach.

DYSTRYBUTOR w Polsce:

alarmnet®

ALARMNET Sp. j.
ul. Rydygiera 12
01-793 Warszawa

tel.: (22) 663 40 85
fax: (22) 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. Rydygiera 12
01-793 Warszawa

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

CDV-71BE

Monitor kolorowy 7" panoramiczny

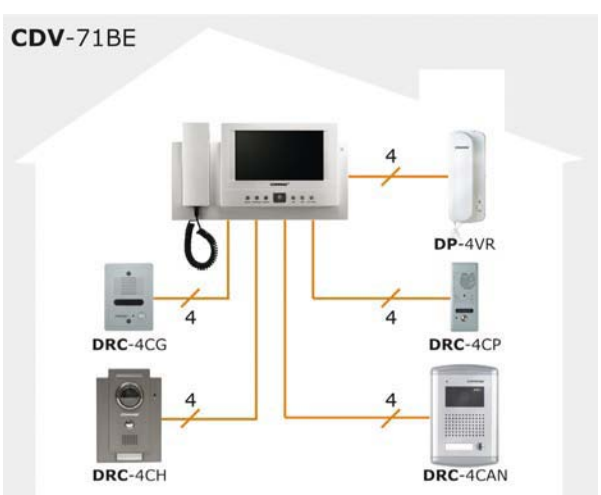
CDV-71BE uzupełnia ofertę monitorów kolorowych firmy GDE Polska. Wyróżnia go 7-calowy, panoramiczny wyświetlacz LCD.

Do monitora możemy podłączyć maksymalnie 4 kamery, więc może on obsługiwać do 4 wejść na posesję. Dodatkowo system wideodomofonowy możemy rozbudować o dodatkowy unifon (DP-4VR) umożliwiający kontakt głosowy z odwiedzającymi nas osobami. Oczywiście pomiędzy monitorem a unifonem możemy nawiązać łączność interkomową.

CDV-71BE posiada wbudowany moduł pamięci, który umożliwia zapis maksymalnie 128 obrazów ze wszystkich podłączonych do monitora kamer.

Charakterystyka monitora:

– monitor kolorowy
– wyświetlacz panoramiczny 7" Color TFT-LCD
– obsługuje cztery wejścia
– możliwość podłączenia dodatkowych monitorów
– funkcja interkomu
– wbudowany moduł pamięci 128 obrazów
– współpracuje z kamerami analogowymi 4-przewodowymi
– zasilanie 230 V



◄ *Przykładowy schemat podłączenia*

Specyfikacja:

Okablowanie	Monitor – kamera: 4 przewody Monitor – unifon: 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

DPV-4RH/DRC-4BG
Monitor głośnomówiący czarno-biały z kamerą

DPV-4RH uzupełnia ofertę firmy GDE POLSKA o monitor głośnomówiący do zastosowań w systemach wideodomofonowych. Monitor współpracuje z kamerami 4-przewodowymi typu DRC-4*** firmy COMMAX (np. DRC-4BG).

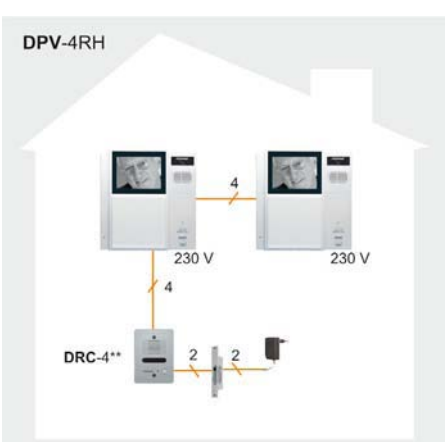
Charakterystyka monitora:

- monitor czarno-biały
- wbudowane głośniki
- kineskop 4", 480 linii
- obsługa jednego wejścia
- możliwość podłączenia dodatkowego monitora
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z kamerami analogowymi czteroprzewodowymi
- zasilanie 230 V

Okablowanie	4 przewody spolaryzowane
Zasilanie	100-240 V AC; 50-60 Hz
Pobór mocy	Czuwanie: 2,5 W Praca: 15 W
Temperatura pracy	od 0°C do 40°C
Wymiary (szer. x wys. x gł.)	211 mm x 226 mm x 52 mm
Masa	1,7 kg

Charakterystyka kamery:

- kamera czarno-biała
- obudowa żeliwna, montaż podtynkowy
- ukryty obiektyw typu PIN-HOLE
- doświetlenie podczerwienią
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z monitorami czteroprzewodowymi
- głębokość tylko 18 mm



Przykładowy schemat podłączenia

GDE POLSKA
Global Distributor of Electronics

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

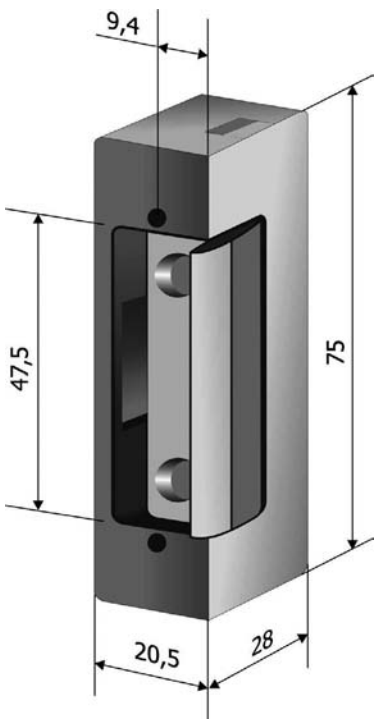
tel./fax: 012 256 50 35, 256 50 25
fax: 012 270 56 96
e-mail: biuro@gde.pl

DOM DES 007

Elektrozaczep symetryczny

Zastosowanie

DES 07 jest elektrozaczepem symetrycznym z regulacją ustawienia zapadki. Przeznaczony jest do współpracy z szyfratorami, czytnikami kart, systemami kontroli dostępu oraz domofonami. Mogą być stosowane w drzwiach metalowych, drewnianych, aluminiowych i PVC. Elektrozaczep DES 07 przystosowany jest do montażu zarówno w drzwiach zewnętrznych i wewnętrznych.



Właściwości

- Symetryczna obudowa
- Regulacja ustawienia zapadki
- Standardowy rozstaw śrub mocujących
- Niski pobór prądu
- 5-letnia gwarancja

Dostępne wersje

Kod Produktu	Nazwa produktu	Pobór prądu przy napięciu zmiennym	Pobór prądu przy napięciu stałym	Cena netto
DES07–12ADU	DES 07 (NC; 12 $V_{AC/DC}$)	300 mA	600 mA	59,00 zł.
DES07P–12ADU	DES 07P (NC z pamięcią; 12 $V_{AC/DC}$)	300 mA	600 mA	64,00 zł.
DES07O–12ADU	DES 07O (NC z odblokowaniem; 12 $V_{AC/DC}$)	300 mA	600 mA	64,00 zł.
DES07OP–12ADU	DES 07OP (NC z odblokowaniem i pamięcią; 12 $V_{AC/DC}$)	300 mA	600 mA	69,00 zł.
DES07N–12-DU	DES 07N (NC niskoprądowy; 12 V_{DC})	–	220 mA	99,00 zł.
DES07NS–12-DU	DES 07NS (NC niskoprądowy z sygnalizacją; 12 V_{DC})	–	220 mA	199,00 zł.
DES07R–12-DU	DES 07R (NO; 12 V_{DC})	–	170 mA	99,00 zł.
DES07RS–12-DU	DES 07RS (NO; z sygnalizacją; 12 V_{DC})	–	170 mA	199,00 zł.
DES07R–24-DU	DES 07R (NO; 24 V_{DC})	–	90 mA	159,00 zł.
DES07RS–24-DU	DES 07RS (NO; z sygnalizacją; 24 V_{DC})	–	90 mA	209,00 zł.

DOM SICHERHEITSTECHNIK

Dom Polska Sp. z o.o.
ul. Krótka 7/9, 42-200 Częstochowa
tel. 034 360 53 64, faks 034 360 53 67
e-mail: dom-dom-polska.pl, www.dom-polska.pl

Kamera serii ICE firmy BAXALL
ICE-CM3H/LV i ICE-CM3H/M

- Kamera kolorowa DSP
- Przetwornik 1/3" CCD
- Wysoka rozdzielczość – 480 TVL

DANE TECHNICZNE	
Przetwornik	1/3" Sony Super HAD CCD
Obróbka obrazu	cyfrowa DSP
Efektywna liczba pikseli	752 (H) x 582 (V)
Czułość	0,7 lx dla obrazu użytecznego z włączoną automatyczną regulacją wzmocnienia (AGC), przysłona obiektywu F1.2
Rozdzielczość	480 TVL
Wyjście wizyjne	1 Vp-p composite video, 75Ω, BNC
Stosunek sygnał/szum	> 50 dB
Balans bieli	2500 K ~ 9500 K
Automatyczna regulacja wzmocnienia (AGC)	28 dB, z możliwością włączenia/wyłączenia
Migawka elektroniczna	1/50 s ~ 1/100 000 s, z możliwością włączenia/wyłączenia
Kompensacja tylnego oświetlenia (BLC)	1 okno konfiguracji (środkowa część obrazu); z możliwością włączenia/wyłączenia
Korekcja gamma	0,45
Synchronizacja	line-lock lub wewnętrzna

OBIEKTYW	
Mocowanie obiektywu	C lub CS
Automatyczna przesłona sterowana sygnałem wideo (video drive)	podłączenie przez 4-wejściowy zacisk z tyłu kamery
Automatyczna przesłona sterowana napięciem DC (DC drive)	4-pinowe, kwadratowe gniazdo z boku kamery; poziom DC jest ustawiany za pomocą potencjometru umieszczonego z tyłu kamery

ZASILANIE	
Wersja niskonapięciowa	24 V AC/50 Hz (od 20,5 V do 32 V); 12 V DC (od 11 V do 14 V)
Wersja sieciowa	od 98 V do 260 V AC/50 Hz
Złącze zasilania	/LV: dwutorowe złącze z tyłu kamery; /M: przewód sieciowy 2 m
Pobór mocy	< 4,2 W
Wskaźnik zasilania	niebieska dioda LED z tyłu kamery

PARAMETRY MECHANICZNE	
Wymiary (dł. x wys. x szer.)	123 x 60 x 52 mm
Masa	/LV: 0,35 kg; /M: 0,5 kg
Obudowa	uchwyt obiektywu odlany z cynku

ŚRODOWISKO PRACY	
Temperatura pracy	-10÷+50°C
Wilgotność względna pracy	20÷80 % (bez kondensacji)
Temperatura przechowywania	-10÷+70°C
Wilgotność względna przechowywania	20÷90% (bez kondensacji)

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

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 Sp. z o.o.
ul. Rydygiera 12
01-793 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. Puławska 597
02-885 Warszawa
tel. (22) 750 89 12
faks (22) 750 89 26
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. Rydygiera 12
01-793 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. Fabryczna 5a
31-553 Kraków
tel. (12) 411 88 88
faks (12) 294 18 88
e-mail: biuro@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

ASSA ABLOY Poland Sp. z o.o.
ul. Warszawska 76
05-092 Łomianki
tel. (22) 751 53 54
faks (22) 751 53 56
biuro@assaabloy.com.pl
www.assaabloy.pl

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. Dworcowa 7
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) 457 68 12, 457 68 32
faks (22) 457 68 95
e-mail: brabork@braborklab.pl
www.braborklab.pl

---

bt electronics
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

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
Arkadiusz Beck
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, 18
faks (22) 855 00 19
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

EUROSAP – LTD Eugeniusz Klowan
ul. Tarniny 28
70-763 Szczecin
tel. (91) 466 60 45, 461 21 50
faks (91) 466 60 46
e-mail: eurosap@go2.pl, eurosap@eurosap.pl
www.eurosap.pl

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

GERARD – Systemy Alarmowe
ul. Suwalska 36d/8
03-252 Warszawa
tel. (22) 675 66 20
faks (22) 674 11 44
e-mail: biuro@alarmy-gerard.pl
www.alarmy-gerard.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.
Al. Jana Pawła II 61/233
01-031 **Warszawa**
tel. (22) 636 13 73, 831 56 81
faks (22) 831 28 52
tel. kom. 693 029 278
e-mail: warszawa@gv.com.pl

ul. Lwowska 74a
33-300 **Nowy Sącz**
tel. (18) 444 35 38, 444 35 39, 444 35 83
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

Inter-Sicherheits-Service Sp. z o.o.
ul. Kobylogórska 2
66-400 Gorzów Wielkopolski
tel. (95) 723 97 77
faks (95) 723 97 82
e-mail: sprzedaz@iss.net.pl
www.iss.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

KABA SECURITY Sp. z o.o.
ul. Połczyńska 51
01-336 Warszawa
tel. (22) 665 88 27
faks (22) 665 88 62
e-mail: kaba@kpw.kaba.com
www.kaba.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

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: handel@laskomex.com.pl
marketing@laskomex.com.pl
www.laskomex.com.pl

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

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

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

NOKTON – DOCZKAL, NIZIO – Sp. J.
ul. Zamorska 41
93-478 Łódź
tel. (42) 250 62 51, 680 08 52
faks (42) 680 08 84
e-mail: info@nokton.com.pl
www.nokton.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.noma2.com.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./faks (71) 343 16 76, 341 78 52, 341 98 54
e-mail: 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 Sp. z o.o.
Zakład Urządzeń Dozymetrycznych
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 Spółka Jawna
W. M. Fredrych, A. Kwiatkowski
ul. Filtrowa 23
87-100 Toruń
tel./faks (56) 660 20 00

PROXIMA Spółka Jawna
W. M. Fredrych, A. Kwiatkowski
Hurtownia Systemów Sygnalizacji Włamania i Napadu

ul. Grudziądzka 11, 87-100 **Toruń**
tel. (56) 661 18 96
tel./faks (56) 661 18 97
e-mail: alarmy@proxima.pl
www.proxima.pl

Oddziały:
Białystok tel. (85) 740 35 35
Częstochowa tel. (34) 361 62 91
Gdańsk tel. (58) 554 83 04
Gdynia tel. (58) 620 69 77
Gliwice tel. (32) 230 47 27
Konin tel. (63) 245 61 61
Kraków tel. (12) 266 62 22
Bydgoszcz tel. (52) 375 41 41
Legnica tel. (76) 854 05 55
Leszno tel. (65) 520 44 67
Łódź tel. (42) 676 72 81
Lublin tel. (81) 745 30 35
Olsztyn tel. (89) 533 86 52
Poznań tel. 0 602 232 159
Rzeszów tel. (17) 857 49 49
Szczecin tel. (91) 482 40 99
Warszawa tel. (22) 838 45 46
Wrocław tel. (71) 333 49 43

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

SECURITY SYSTEM INTEGRATION Sp. z o.o.
ul. Irysowa 4
55-040 Bielany Wrocławskie
tel. (71) 311 04 30
faks (71) 311 28 63
e-mail: ssi@ssi-tv.pl
www.ssi-tv.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

PHS SOFTEX DATA
ul. Poleczki 47
02-822 Warszawa
tel. (22) 331 19 90
faks (22) 331 15 11
e-mail: softex@softex.com.pl
www.softex.com.pl

SOLAR 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. Winogrady 10
61-663 **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

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 SYSTEMY BEZPIECZEŃSTWA
ul. A. Dauna 70
30-629 Kraków
tel. (12) 655 85 85
faks (12) 425 63 68
e-mail: talcomp@talcomp.pl
www.talcomp.pl

TAYAMA POLSKA Sp. J.
ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, (32) 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

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

– 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 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

TRIKON
32-447 Siepraw 1123
tel. (12) 274 61 27
faks (12) 274 51 51
e-mail: biuro@trikon.com.pl
www.trikon.com.pl

TYCO FIRE AND INTEGRATED SOLUTIONS Sp. z o.o.
ul. Żupnicza 17
03-821 Warszawa
tel. (22) 518 21 00
faks (22) 518 21 01
e-mail: tycofis-pl@tycoint.com
www.tycofis.pl

UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. (12) 398 99 00
faks (12) 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

Oddziały:
ul. Ratuszowa 11, 03-450 **Warszawa**
tel. (22) 619 22 04
faks (22) 818 64 67

Os. Polan 33, 61-249 **Poznań**
tel. (61) 872 92 08 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 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 Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. (61) 878 13 00
faks (61) 878 13 82
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
2M Elektronik	-	TAK	TAK	TAK	-
3D	TAK	TAK	-	-	TAK
4 COM	-	TAK	TAK	TAK	TAK
AAT Trading Company	-	TAK	TAK	-	TAK
ACIE	TAK	-	TAK	TAK	TAK
ACSS	-	-	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
ASSA ABLOY Poland	-	-	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	-	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	-
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	-
Eurosap – LTD	-	TAK	TAK	TAK	-
FES	TAK	TAK	TAK	TAK	-
Gerard Systemy Alarmowe	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	-

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Intel	-	TAK	TAK	TAK	TAK
Ired	TAK	TAK	TAK	TAK	-
ISS	TAK	-	-	-	-
Janex International	-	-	TAK	-	TAK
Kaba Security Sp. z o.o.	TAK	TAK	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
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	-	-	-	-
Micronix	-	TAK	TAK	-	-
Miwi-Urmet	TAK	TAK	TAK	-	TAK
Nokton Sp. J.	TAK	-	-	-	-
Noma 2	-	TAK	-	TAK	-
NORBAIN Polska	TAK	-	TAK	-	TAK
OBIS Sp. J.	-	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	-	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	-
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 Sp. z o.o.	-	TAK	TAK	-	TAK

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
2M Elektronik	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
3D	-	TAK	-	-	-	-	-	-	-
4 COM	TAK	TAK	TAK	TAK	-	TAK	TAK	TAK	-
AAT Trading Company	TAK	TAK	TAK	TAK	-	TAK	TAK	-	-
ACIE	TAK	-	TAK	-	-	-	-	-	-
ACSS	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	-	-	-
ASSA ABLOY Poland	-	-	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
bt electronics	-	-	TAK	-	-	TAK	-	TAK	-
C&C Partners	-	TAK	-	-	-	-	TAK	-	-
CAMSAT	-	TAK	-	-	-	-	-	-	-
CBC Poland	-	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
CONTROL SYSTEM FMN	TAK	TAK	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
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	-	-
Eurosap LTD	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
FES	TAK	TAK	TAK	TAK	-	-	-	-	TAK
Gerard Systemy Alarmowe	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

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	-	-
ISS	-	-	-	-	-	-	-	TAK	-
Janex International	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
Kaba Security Sp. z o.o.	TAK	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	TAK	TAK	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
MicroMade	-	-	TAK	-	Rejestracja czasu pracy			-	-
Micronix	TAK	TAK	TAK	TAK	-	-	-	TAK	-
Miwi-Urmet	TAK	TAK	TAK	-	TAK	TAK	-	-	-
Nokton Sp. J.	TAK	-	-	-	-	-	TAK	-	-
Noma 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
NORBAIN Polska	-	TAK	-	-	-	TAK	-	-	-
OBIS Sp. J.	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	-
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	-	-	-	-	-	-	-
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 Sp. z o.o.	-	-	-	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
Daniel Kamiński
Sławomir Wagner
Marcin Pyclik
Dział DTP
Jarosław Witkowski
jarek@zabezpieczenia.com.pl
Korekta
Izabela Jesiołowska
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
Poligrafus
ul. Oszmiańska 9
03-503 Warszawa
tel. (22) 679 28 18

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

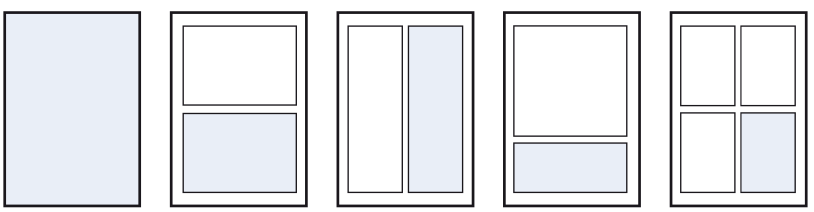
jednorazowy wpis	– 60 zł

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
200 x 282 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

24M.pl	71	Gunnebo	65	Roger	66
AAT-T	59, 72, 80	HID	108	Satel	27
ACSS	84, 85	Kabe	32	Suma	70
ADD	78	Laskomex	52	Techom	76
Alarmnet	41	Miwi-Urmet	2	Trikon	61
Alpol	53	MTK	86	Visonic	35
C&C Partners	63	Polon-Alfa	1		
CBC Poland	107	Protector Polska	62		

GANZ®

technologia
jutra
już dziś

REJESTRATOR CYFROWY
ZR-DHC1630NP

ZR-DHC1630NP
to najnowocześniejsze rozwiązanie dla wymagających systemów CCTV. Zapewnia najwyższą jakość monitoringu wizyjnego o niespotykanej efektywności i skalowalności.

- Przyjazny użytkownikowi, intuicyjny Graficzny Interfejs Użytkownika
- 16 kanałów video + 16 kanałów audio, rejestracja w rozdzielczości D1
- Port Gigabit Ethernet oraz seria zaawansowanych aplikacji GMS do zarządzania systemem
- Interfejs ATM/POS do współpracy z bankomatami i systemami kasowymi
- Inteligentne wyszukiwanie nagrań m.in. na podstawie analizy zmian obrazu

więcej informacji na stronie: www.cbcpoland.pl

CBC GROUP
CBC (POLAND) Sp. z o.o.

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