CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 4(86)/2012

ZABEZPIECZENIA

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

W NUMERZE:

ZOBACZ

ZAPISZ

POKAŻ

ZŁAP

iPOLiS

Rozwiązania sieciowe firmy Samsung

Obraz w rozdzielczości Full HD	Inteligentna Analiza Obrazu	Skalowalna rejestracja	Zdalny podgląd i sterowanie
FULL HD			

Rozwiązania Samsung HD network security generują nawet pięciokrotnie więcej detali obrazu w porównaniu z systemem o standardowej rozdzielczości. Generowanie obrazu HD, rejestrowanie oraz wyświetlanie połączono w jednym systemie bezpieczeństwa, pozwalającym uzyskać niewiarygodnie wysoki poziom odwzorowania szczegółów obrazu.

Kamery HD oraz monitory generują obrazy w formacie 16:9 i pozwalają operatorom określić z maksymalną dokładnością specyficzne obszary zainteresowania do bliższego zbadania – bez strat rozdzielczości i bez efektu „pikselacji" przy obserwacji. A dzięki zapisowi w rozdzielczości HD na materiale zarejestrowanym można wszystko zobaczyć z tą samą jakością.

Z pełnym zestawem kamer, wyborem opcji sprzętowych lub oprogramowania oraz monitorami HD, możesz stworzyć system bezpieczeństwa idealnie dopasowany do twoich potrzeb.

Sieciowe rozwiązania bezpieczeństwa Samsung HD.
Inteligentniejsze bezpieczeństwo.

E **STEsecurity@samsung.com**

Samsung Techwin Europe Ltd
Address: Postępu 15 C, 02-676 Warszawa
Tel: +48 222 050 777
Fax: +48 222 050 763

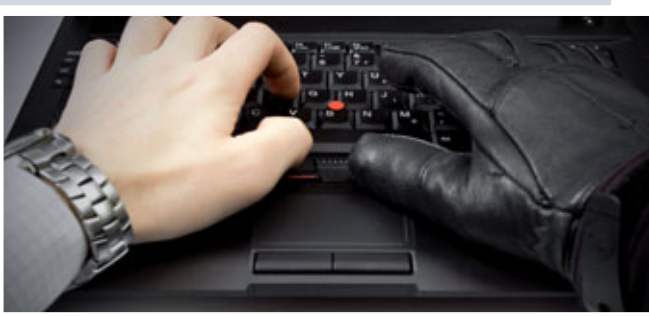
SAMSUNG

Spis treści

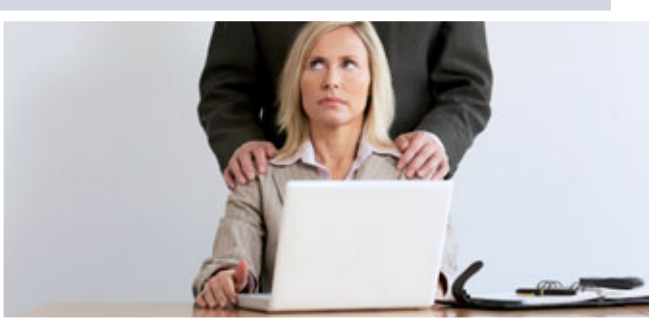
CZASOPISMO ZABEZPIECZENIA 4/2012

Kompleksowe układy chroniące systemy CCTV przed przepięciami **26**

Nowe spojrzenie na ochronę informacji niejawnych (cz. 2) **52**



Socjotechnika **60**



Kontrolowanie pracownika **68**

Axon Video IP Protector 4 PoE +

Firma **HSK DATA**, producent profesjonalnych ochronników przeciwprzepięciowych, oferuje nowe zabezpieczenia do urządzeń zasilanych metodą PoE +.

Najnowszy model **AXON Video IP Protector 4 PoE +** jest wielokanałowym ochronnikiem obsługującym równocześnie cztery kamery cyfrowe o zwiększonym poborze zasilania. Standard PoE + pozwala na zasilanie urządzeń z wykorzystaniem napięcia dochodzącego do 120 V_{DC}. Oprócz toru zasilania AXON Video IP Protector 4 PoE + zabezpiecza równocześnie tor transmisji danych.

Ochronnik umożliwia transfer danych z prędkością 10/100/1000 Mb/s, a zastosowane ochronniki gazowe są w stanie – przy odpowiednim uziemieniu – odprowadzić duże prądy udarowe o wartości maksymalnej dochodzącej do 5 kA.

Parametry ochronne urządzenia spełniają wymagania normy PN EN 614643-21.

Bezpośr. inf. Wojciech Zieliński
HSK DATA

Samsung wprowadza kompaktowy, czterokanałowy rejestrator cyfrowy H.264 z wbudowanym ekranem dotykowym LCD

Najnowszy rejestrator cyfrowy z serii SRD firmy **Samsung**, model **SRD-442**, jest przeznaczony do zastosowania w niewielkich firmach, biurach oraz lokalach mieszkalnych. Jest niedrogi i pozwala zaoszczędzić przestrzeń dyskową.

Kompaktowy model SRD-442 to czterokanałowy rejestrator DVR z wbudowanym 4,3-calowym monitorem dotykowym LCD, który umożliwia łatwy podgląd bieżących obrazów pochodzących z kamer bądź nagrań odtwarzanych z dysku. SRD-442 może nagrywać obrazy w rozdzielczościach od CIF do 4CIF w trybie standardowym i alarmowym.

W razie potrzeby SRD-442 może przesłać obraz do zewnętrznego monitora, jednakże wbudowany 4,3-calowy ekran dotykowy LCD, o rozmiarach porównywalnych do rozmiarów ekranów telefonów serii Galaxy S, jest wystarczająco duży, aby dyskretnie obserwować dowolne zdarzenia. Pozwala on także swobodnie nawigować poprzez 22-językowe menu ekranowe.

– Pomimo atrakcyjnej ceny SRD-442 nie ustępuje jakością innym rejestratorom i ma wiele bardzo użytecznych i technicznie zaawansowanych funkcji – powiedział **Peter Ainsworth**, Senior Product Manager w Samsung Techwin Europe. *– Przykładowo, rejestrator wykorzystuje kompresję H.264 w celu zmaksymalizowania liczby nagrań wizyjnych, które mogą być przechowywane na wewnętrznych dyskach SATA, a jego użytkownicy mogą zdalnie przeglądać bieżące obrazy z kamer bądź nagrania odtwarzane z dysku poprzez urządzenia typu smartphone lub tablet, wykorzystując bezpłatne aplikacje Samsung iPOLiS. SRD-442 może również sterować pracą kamer PTZ RS-485 za pomocą różnych protokołów, np. Panasonic czy Pelco D lub P.*

SRD-442, o wymiarach zaledwie 215 mm x 88 mm x 350 mm, umożliwia nagrywanie dźwięku na dowolnym z czterech kanałów fonicznych oraz posiada dwa porty USB umożliwiające tworzenie kopii zapasowych i eksportowanie zarejestrowanego materiału wizyjnego.

Seria rejestratorów cyfrowych SRD firmy Samsung składa się z ponad 20 modeli w wersjach cztero-, ośmio- i szesnastokanałowych. Każdy z nich korzysta z nowoczesnej kompresji H.264, która minimalizuje wymagania dotyczące pasma sieciowego. Wszystkie modele mają identyczny intuicyjny graficzny interfejs użytkownika (GUI), który ułatwia operatorom dobór właściwej poklatkowości i rozdzielczości rejestrowanych obrazów, a ponadto mogą być obsługiwane za pomocą zdalnego, bezpłatnego oprogramowania Samsung NET-i Viewer.

Bezpośr. inf. David Solomons
DRS Marketing

Nowy pulpit dyskusyjny do systemu konferencyjnego DCN Next Generation firmy Bosch

System konferencyjny **DCN Next Generation** firmy **Bosch** łączy eleganckie wzornictwo z doskonałą jakością dźwięku i funkcjonalnością dostosowaną do indywidualnych potrzeb klienta.

Opływowe kształty oraz eleganckie połączenie ponadczasowej matowej czerni ze srebrem gwarantuje idealne dopasowanie pulpitu dyskusyjnego DCN-D do wystroju każdej sali konferencyjnej.

Przyciski na pulpicie są duże, a ich układ zapewnia intuicyjne i komfortowe użytkowanie. Nawet mniej doświadczone osoby szybko opanują zasady obsługi urządzenia.

Wszystkie pulpity dyskusyjne są wyposażone w głośnik, mikrofon, który można aktywować jednym przyciskiem, oraz złącze słuchawkowe z regulacją głośności. Każdy pulpit można skonfigurować w taki sposób, aby pełnił rolę pulpitu przewodniczącego konferencji. Dzięki temu przewodniczący może kontrolować przebieg konferencji, rejestrując prośby o udzielenie głosu oraz udzielając głosu wybranemu uczestnikowi.

W ofercie dostępnych jest pięć wersji pulpitu dyskusyjnego. Wersja podstawowa z mikrofonem podłączonym na stałe umożliwia wypowiadanie się i przysłuchiwanie się konferencji. Kolejne wersje to pulpit z gniazdem do podłączenia mikrofonu, pulpit z funkcją głosowania oraz pulpit z selektorem kanałów do obsługi tłumaczeń symultanicznych (maksymalnie 31 języków). Organizatorzy spotkań mogą więc dopasować środowisko konferencyjne do swoich indywidualnych wymagań.

Bezpośr. inf. Bosch Security Systems

Ochronnik AXON PoE Spliter Protector od HSK DATA

Ochronnik **AXON PoE Spliter Protector** to nowy ochronnik przeciwprzepięciowy w ofercie firmy **HSK DATA**, który zapewnia profesjonalne zabezpieczenie przeciwprzepięciowe toru transmisyjnego przenoszącego także napięcie zasilające zgodnie ze standardem PoE i umożliwia łączenie lub rozdzielanie sieci LAN i napięcia zasilającego.

W praktyce oznacza to, że wszędzie tam, gdzie dotychczas stosowano dwa oddzielne urządzenia, będzie można zastosować jeden ochronnik AXON PoE Spliter Protector, a tym samym ograniczyć koszty inwestycji. Ochronę przeciwprzepięciową zapewniają gazowe elementy odgromowe, które przy odpowiednim uziemieniu są w stanie odprowadzić ładunek zakłócający. W torze zasilania zastosowano także elementy półprzewodnikowe, które chronią urządzenie przed przepięciami międzyliniowymi. W celu zwiększenia obciążalności toru zasilania zwarto pary przewodów 4 i 5 oraz 7 i 8. Warunkiem poprawnej pracy urządzenia jest podłączenie go do odpowiedniego uziemienia lub przewodu ochronnego PE sieci elektrycznej. Rezystancja uziemienia bądź skuteczność zerowania powinny być zgodne z obowiązującymi przepisami.

Bezpośr. inf. Wojciech Zieliński
HSK DATA

JVC poszukuje rywala

Firma **Euroalarm**, autoryzowany dystrybutor marki **JVC** w Polsce, przedstawiła na tegorocznych targach Securex rodzinę nowych kamer **Super LoLux HD2**. Teraz mamy przyjemność przedstawić najmłodszego przedstawiciela z tej serii – model **VN-H157WPU**. Kamera ta może pracować w różnych warunkach i można ustawiać ją w różnych pozycjach. Ponadto ma wszystkie inne atuty serii Super LoLux HD2. Gdy pod koniec 2011 roku otrzymaliśmy informację o tym, że w drugim kwartale 2012 roku zostaną wprowadzone wspomniane nowości, liczyliśmy na to, że będą zdrowo konkurować z produktami firmy Sanyo, ale firma ta wycofała swoją linię konkurencyjnych urządzeń, dlatego czekamy na innego godnego rywala. Pomimo zaawansowanych rozwiązań firma JVC utrzymała poziom cen byłego konkurenta.

Kamery Full HD z serii Super LoLux HD2 mogą być stosowane przy słabym oświetleniu bez dodatkowych oświetlaczy. Ich wysoką czułość można wykazać dzięki prostemu doświadczeniu – umieszczając w ciemnym pomieszczeniu ścienny zegar z sekundnikiem. Płynny ruch wskazówki sekundnika pokazuje, że czytelność ekspozycji nie została osiągnięta dzięki naświetlaniu przez dłuższy czas, lecz dzięki nowatorskiej obróbce obrazu w procesorze DSP. Nawet oświetlenie na poziomie 0,3 lx pozwala na reprodukcję kolorów, co niejednokrotnie umożliwi identyfikację obserwowanych obiektów. Osiągnięto także wysoki stopień kompresji. Metoda DSP H.264 High Profile Super LoLux, w odróżnieniu od popularnych kompresji H.264 Main Profile i H.264 Baseline Profile, umożliwia dystrybucję obrazu o wysokiej rozdzielczości z jednoczesnym oszczędnym wykorzystaniem pasma sieciowego. JVC H.264 High Profile nie zapewnia jednakowej kompresji dla całego kadru, lecz uwzględnia nasycenie poszczególnych fragmentów szczegółami. Fragmenty obrazu z dużą ilością szczegółów są słabiej kompresowane, a fragmenty jednolite – silniej. Kolejne narzędzie, jakie mamy do dyspozycji, to funkcja inteligentnej obróbki obrazu CLVI. W przypadku scen mało kontrastowych (mgła, smog)

narzędzie to pozwala na wyostrzenie krawędzi i cyfrowe usunięcie niepożądanych efektów. Funkcja ta skutecznie kompensuje silne, punktowe światło, np. z reflektorów samochodów, a szeroki zakres dynamiki zapewnia doskonałe odwzorowanie scen prześwietlonych i niedoświetlonych. Kamera VN-H157WPU jest wyposażona w obiektyw zmiennoogniskowy (3–9 mm) oraz opatentowany samokontrujący mechanizm ślimakowy do precyzyjnej zmiany ogniskowej z dokładnością 0,01 mm.

Kamery sieciowe produkcji JVC są obsługiwane przez oprogramowanie systemowe wielu producentów, między innymi Alnet Systems, Milestone, See Tec, Siemens, Axxon, Nuuo. Otwarte oprogramowanie w standardzie ONVIF gwarantuje pełną interoperacyjność pod warunkiem zaimplementowania całego SDK (kodów źródłowych). Oprogramowanie Milestone Xprotect Enterprise jest standardowo na wyposażeniu rejestratorów JVC VR-X1600U (obsługujących 16 kamer) i VR-X3200U (obsługujących 32 kamery). Na targach Securex kamery Super LoLux HD2 współpracowały już z najnowszą wersją oprogramowania Alnet Systems.

Kamery z serii Super LoLux HD2 oferują dwukierunkową transmisję dźwięku i alarm sabotażowy, mają obudowę o stopniu szczelności IP66 i przetwornik CMOS 1/3" wytwarzają 30 kl./s przy rozdzielczości Full HD i kompresji H.264.

Należy podkreślić bardzo dobry średni czas bezawaryjnej pracy (MTBF) kamer IP firmy JVC wynoszący 90000 godzin (ponad 10 lat).

Bezpośrednia inf. Waldemar Kulik
I.T.O.M. Euroalarm

Gwarancja pełnej kontroli z nowym cyfrowym rejestratorem wizyjnym firmy Bosch

Firma **Bosch** powiększa ofertę cyfrowych rejestratorów wizyjnych serii 600 i wprowadza na rynek model **DVR 670** – zawarte w jednej kompaktowej jednostce urządzenie służące do zarządzania sygnałem wizyjnym.

Rejestrator DVR 670 wykorzystuje wydajną metodę kompresji H.264, która gwarantuje doskonałą jakość obrazu przy relatywnie niskich wymaganiach dotyczących szerokości pasma i pojemności dysku. Dzięki temu możliwy jest zapis obrazów o rozdzielczości 4CIF z 16 kanałów wizyjnych równocześnie, w czasie rzeczywistym.

Systemem można zarządzać lokalnie – z wykorzystaniem klawiatury Bosch IntuiKey, myszy, pilota zdalnego sterowania na podczerwień – lub bezpośrednio – za pomocą panelu przedniego urządzenia. Wszystkie modele rejestratorów serii 600 są wyposażone w klawiaturowe złącza przelotowe, więc za pomocą pojedynczej klawiatury IntuiKey można obsługiwać aż 16 rejestratorów.

Model DVR 670 oferuje też szereg opcji zdalnego zarządzania (za pośrednictwem sieci Ethernet), które zapewniają podgląd materiału wizyjnego, dostęp do archiwum, sterowanie wieloma rejestratorami oraz możliwość ich konfiguracji. Funkcje te są zaimplementowane w oprogramowaniu Bosch Control Center oraz Bosch Video Client.

Ponadto dostęp do urządzenia jest możliwy z poziomu przeglądarki internetowej. Oferowana jest też aplikacja dostosowana do urządzeń mobilnych, która umożliwia podgląd i sterowanie kamerami obrotowymi za pomocą urządzeń iPhone, iPad lub iPod. Aplikacja DVR Viewer umożliwia zdalny podgląd na żywo oraz sterowanie kamerami obrotowymi.

W przypadku pobudzenia wejścia alarmowego rejestratora DVR 670 może wysłać pocztą e-mail 10-sekundowy wideoklip dodawany automatycznie do powiadomienia alarmowego.

Operatorzy z pewnością docenią także funkcje usprawniające pracę, na przykład inteligentne wyszukiwanie (*Smart Search*), które umożliwia szybkie odnajdywanie zdarzeń w zarejestrowanym materiale wizyjnym.

Nowy rejestrator DVR 670 chroni najważniejsze nagrania przed przypadkowym nadpisaniem. Cały zapis zawiera cyfrowe znaczniki autoryzujące, które gwarantują wiarygodność nagrań, a oprogramowanie odtwarzające materiały archiwalne umożliwia przeglądanie nagrań na dowolnym komputerze.

Bardzo prosta instalacja oraz intuicyjna obsługa DVR 670 sprawiają, że użytkownik nie potrzebuje specjalnego przeszkolenia. Po podłączeniu urządzenia należy tylko wybrać język, ustawić datę i godzinę, a zapis rozpocznie się automatycznie. Istotną zaletą rejestratora jest wysoka niezawodność jego działania, która obniża ogólny koszt eksploatacji.

Nowe urządzenie służące do zarządzania sygnałem wizyjnym doskonale sprawdzi się w małych obiektach, w szkołach, sklepach, bankach czy hotelach, a także w zlokalizowanych w różnych miejscach budynkach należących do jednego przedsiębiorstwa.

DVR 670 jest dostępny w wersjach o różnych pojemnościach pamięci dyskowej. Można też zamówić model z wbudowaną nagrywarką DVD.

Bezpośr. inf. Bosch Security Systems

Nowy system JABLOTRON 100

W maju 2012 **JABLOTRON ALARMS** wprowadził na polski rynek nowy system alarmowy – **JA-100**. Celem producenta było opracowanie rozwiązania, które zapewni zarazem wysoki poziom bezpieczeństwa oraz intuicyjność obsługi.

Aby to osiągnąć, opracowano nową serię klawiatur i czytników zbliżeniowych z opatentowaną funkcją sterowania za pomocą dołączanych segmentów. Trzy kolory oznaczają trzy różne stany pracy.

JA-100 wykorzystuje czterożyłową magistralę cyfrową. Podstawowe parametry nowej centrali to 120 adresów dla urządzeń bezprzewodowych i magistralowych, 15 niezależnych stref, 32 programowalne wyjścia. Wraz z nowym systemem JABLOTRON przygotował bogatą ofertę urządzeń peryferyjnych, magistralowych oraz bezprzewodowych. Dodatkowym atutem jest również nowoczesny wygląd oferowanych produktów.

Firma JABLOTRON ALARMS oraz dystrybutorzy krajowi – **DPK System** i **JabloTech** – przygotowali serię szkoleń dotyczących nowego systemu.

Najbliższe terminy szkoleń:
– 11 września 2012 r. (Gdańsk),
– 27 września 2012 r. (Łódź),
– 9 października 2012 r. (Wrocław),
– 25 października 2012 r. (Lublin),
– 14 listopada 2012 r. (Warszawa).

Szczegółowe informacje dotyczące szkoleń znajdą państwo na stronie *www.jablotronalarms.pl*.

Bezpośr. inf. JABLOTRON ALARMS

PR102DR – prosty i tani kontroler dostępu w ofercie firmy ROGER

W ofercie firmy **ROGER** pojawił się nowy kontroler do obsługi pojedynczego przejścia w systemie kontroli dostępu **RACS 4**. Urządzenie powstało na bazie popularnego kontrolera PR402DR poprzez uproszczenie jego konstrukcji oraz usunięcie rzadziej stosowanych funkcji. Kontroler **PR102DR** ma najistotniejsze możliwości kontrolera **PR402DR**, a jednocześnie jest tańszy i łatwiejszy w konfiguracji.

Podstawowe cechy nowego urządzenia to:
– zasilanie napięciem $12V_{DC}$,
– przekaźnik 5 A/30 V,
– dwie programowalne linie wejściowe NO/NC,
– jedna programowalna linia wyjściowa,
– możliwość podłączenia dwóch czytników serii PRTxxLT na karty EM 125 kHz,
– obsługa do 4000 użytkowników,
– bufor pamięci o pojemności do 32 000 zdarzeń.

Nowy kontroler jest dostępny w dwóch wersjach – jako moduł w obudowie z tworzywa sztucznego do montażu na standardowej szynie DIN 35 mm (oznaczenie PR102DR) oraz jako moduł PCB (oznaczenie PR102DR-BRD).

Możliwe jest tworzenie prostych instalacji kontroli dostępu z wykorzystaniem wyłącznie kontrolerów PR102DR, jak również stosowanie ich wraz z innymi kontrolerami ROGER w celu pełnego wykorzystania zróżnicowanych możliwości dostępnych urządzeń.

Bezpośr. inf. Kamil Stadnicki
ROGER

Integracja kamer i rejestratorów Samsung z oprogramowaniem VMS niezależnych firm

Samsung ogłosił, że przyspieszył program integrowania swoich kamer oraz rejestratorów DVR i NVR z systemami zarządzającymi oferowanymi przez wiodących, niezależnych producentów oprogramowania.

Na liście firm oferujących „otwarte" oprogramowanie VMS, z którymi Samsung współpracuje ze względu na możliwość integracji sprzętu i systemów pochodzących od różnych wytwórców, znalazły się między innymi firmy: Axxon, Aimetis, Alnet Systems, Digifort, Griffid, Ipronet, Exacq, Genetec, ISS, Luxriot, Milestone, Mirasys, ONssi i Seetec.

– Klienci z całej Europy mają zaufanie do marki Samsung, a dzięki temu, że oferujemy zarazem analogowe, sieciowe oraz hybrydowe rozwiązania z zakresu dozoru wizyjnego, często korzystają z różnych naszych produktów jednocześnie – powiedział **Tim Biddulph**, IP Product Manager w Samsung Techwin Europe. *– Zdajemy sobie jednak sprawę z tego, że w tak trudnych jak obecne warunkach ekonomicznych musimy umożliwić klientom osiągnięcie maksymalnych korzyści wynikających z poczynionych przez nich inwestycji. To z kolei oznacza, że musimy umożliwić połączenie urządzeń marki Samsung z produktami innych firm. Bliska współpraca z firmami produkującymi aplikacje VMS wynika z naszej filozofii Smart Security i chodzi w niej przede wszystkim o ułatwienie klientom stopniowego zastępowania istniejących systemów analogowych rozwiązaniami IP. Funkcjonalność oprogramowania VMS różnych firm z pewnością nie będzie identyczna, jednakże bez względu na wybrany rodzaj platformy klient może oczekiwać zarówno wysokiego stopnia kontroli nad pracą kamer i rejestratorów różnych producentów, jak i elastyczności w integrowaniu urządzeń i funkcji. Oczywiście informujemy wszystkich naszych klientów o tym, o jakie funkcje i możliwości powinni pytać dostawców oprogramowania VMS, zanim podejmą decyzję co do wyboru określonego rozwiązania.*

Bezpośr. inf. David Solomons
DRS Marketing

Videotec powiadomił o powołaniu Gianluki Bassana na stanowisko Marketing Managera

By umocnić i tak silną pozycję firmy **Videotec**, która już teraz jest obecna na rynkach na trzech kontynentach, nowy Marketing Manager podejmie strategiczne działania w celu powiększenia oferty i dotarcia na nowe rynki.

Gianluca Bassan ma 32 lata i jest specjalistą w dziedzinie sprzedaży i marketingu. Dotychczas pracował w dziale zajmującym się rozwijaniem najnowszych technologii związanych z cyfrową telewizją dozorową.

W notatce opublikowanej przez firmę Videotec podkreśla się rynkowe podejście Gianluki Bassana, które w połączeniu z pasją i doświadczeniem pozwoli na wprowadzenie na rynek wielu innowacyjnych produktów.

Bezpośr. inf. Martina Panighel
Videotec SpA
Tłumaczenie: Redakcja

Xpanse Video Wall – najnowszy system ścian wideo

Amerykańska firma **Aventura Technologies** wprowadziła na rynek najnowszy system ścian wizyjnych **Xpanse Video Wall**. Jest on gotowym do użycia produktem, nie wymagającym skomplikowanej konfiguracji. Łatwy w obsłudze interfejs nie ogranicza w żaden sposób jego funkcjonalności.

Zestaw składa się ze sterownika posiadającego złącza USB, VGA, HDMI, DVI, BNC, S-Video, Ethernet i maksymalnie 40 monitorów (plazmowych, LCD lub projektorów) o przekątnej od 38 do 110 cali.

Sterownik działa w środowisku Windows i dzięki oprogramowaniu Xpanse Control odbiera dane od operatorów i z podłączonych kamer, konwertuje je oraz wyświetla na monitorach. Ponadto oprogramowanie Xpanse Client, zainstalowane na zdalnych komputerach operatorów, pozwala zarządzać zawartością ściany wizyjnej przez sieć LAN. Operator może dowolnie dostosowywać wyświetlane treści i zarządzać rozmiarami obrazów. Co więcej, ściana wizyjna może być obsługiwana przez kilku użytkowników jednocześnie. Mogą oni wyświetlać obraz będący kopią tego, co widzą na swoich lokalnych pulpitach, umieszczać ten obraz na dowolnym obszarze na ścianie wizyjnej, uruchamiać aplikacje sterownika. Dzięki innowacyjnej funkcji MultiMouse każdy z nich ma możliwość wyświetlenia kursora o wybranym kolorze. Sercem sterownika jest wydajny sześciordzeniowy procesor Intel Xeon, który obsługuje pamięć RAM o maksymalnej pojemności 24 GB.

Xpanse Video Wall jest pierwszym tego typu systemem w branży zabezpieczeń, przygotowanym do obsługi zarówno kamer analogowych, jak i kamer IP.

Więcej informacji na temat systemu Xpanse Video Wall można uzyskać u wyłącznego polskiego dystrybutora, którym jest firma **ZBAR** z Łodzi (*www.zbar.com.pl*).

Bezpośr. inf. Krystian Witczak, Karolina Zasada
ZBAR

Samsung wprowadza linię kamer sieciowych 4CIF z funkcją WDR

Nowa linia kamer sieciowych **Samsung 4CIF** z funkcją WDR została opracowana jako rozwiązanie alternatywne i konkurencyjne cenowo względem kamer megapikselowych, z myślą o nadzorze wizyjnym, w którym wymagana jest wysoka jakość obrazów.

Szkoły, szpitale, biura, fabryki, hurtownie i sklepy to tylko niektóre obiekty, w których warto zainstalować urządzenia o rozdzielczości 4CIF z nowej linii produktowej, na którą składają się: kamera **SNB-3002** w standardowej obudowie, kamera kopułkowa **SND-3082**, kamera kopułkowa **SND-3082F** do montażu w suficie podwieszanym oraz wandaloodporna kamera kopułkowa **SNV-3082**.

Linię kamer o rozdzielczości 4CIF wyposażono w funkcję *Power over Ethernet* (zasilanie przez Ethernet), która zmniejsza koszty instalacji dzięki zasilaniu i transmisji obrazu/dźwięku poprzez pojedynczy kabel sieci Ethernet. Nowa seria kamer oferuje również wielostrumieniowość, wybór metod kompresji (MJPEG, MPEG-4 lub H.264), a także zapewnia jednoczesny przesył obrazów do różnych lokalizacji przy zróżnicowanej prędkości transmisji (do 25 kl./s) i w różnej rozdzielczości. Umożliwia to poszczególnym upoważnionym użytkownikom monitorowanie w czasie rzeczywistym w jednym miejscu przy równoczesnym zapisie obrazów w innej lokalizacji. W tym samym czasie obrazy mogą zostać dodatkowo zapisane na opcjonalnej karcie pamięci SD i być oglądane na żywo na urządzeniu mobilnym (np. tablecie lub smartfonie). Możliwe jest powiadamianie pocztą elektroniczną o zaistniałych zdarzeniach alarmowych.

Nowe modele kamer sieciowych o rozdzielczości 4CIF zostały wyposażone w procesor DSP serii A1 firmy Samsung i mają funkcję WDR, dlatego można je zainstalować w miejscach o dużym zróżnicowaniu poziomów oświetlenia.

Wszystkie cztery modele mają funkcję pracy dzienno-nocnej z mechanicznym filtrem podczerwieni oraz przetwornik CCD, który umożliwia generowanie kolorowych obrazów o wysokiej jakości przy minimalnym oświetleniu na poziomie 0,001 luksa w trybie pracy ze spowolnioną migawką typu *sens-up* oraz obrazów monochromatycznych przy oświetleniu 0,0001 luksa, także w trybie pracy ze spowolnienioną migawką.

Kamery Samsung 4CIF mają funkcję wykrywania zmiany kadru, która generuje alarm na przykład w przypadku zabrudzenia obiektywu farbą lub w razie zmiany pola widzenia kamery. Dwukierunkowy tor akustyczny zapewnia pełną komunikację głosową.

Dwanaście indywidualnych, wielokątnych stref prywatności umożliwi na przykład to, że okna w mieszkaniu nie będą objęte monitoringiem, natomiast funkcja cyfrowej stabilizacji obrazu DIS (ang. *Digital Image Stabilization*) niweluje wstrząsy kamery przy silnym wietrze lub w przypadku wibracji konstrukcji mocującej.

Bezpośr. inf. David Solomons
DRS Marketing

Nowe rejestratory CNB HDx serii E

Firma **CNB** wprowadziła do sprzedaży nową serię rejestratorów. Uzupełniła w ten sposób swoją ofertę o tańsze urządzenia, które pomimo przystępnej ceny realizują wiele ciekawych funkcji. Do serii tej należą rejestratory **HDF1212E** (czterokanałowy), **HDE2424E** (ośmiokanałowy) oraz **HDS4848E** (szesnastokanałowy). Bardzo użyteczną cechą jest niezależna obsługa wyjść BNC oraz VGA, tzw. Dual Display, dzięki której na jednym monitorze możemy wyświetlać obraz w trybie na żywo, a na drugim przeglądać nagrania. Inna opcja to wyświetlanie prezentacji albo reklam (wgrywanych przez interfejs USB) na jednym monitorze z zachowaniem możliwości normalnej obsługi rejestratora na drugim monitorze. Rejestrator może wytwarzać trzy strumienie wizyjne – jeden służący do zapisu obrazów na dysk, drugi do pracy w sieci, a trzeci do pracy na urządzeniach mobilnych. Ponadto możliwy jest też zdalny podgląd obrazów przesyłanych na żywo z innego rejestratora. Dla każdego strumienia możemy ustawić odpowiednią ilość klatek na sekundę, stopień kompresji oraz rozdzielczość, dzięki czemu możemy dopasować wielkość strumienia wizyjnego do przepustowości sieci. Warto także zwrócić uwagę na dostępność oprogramowania **iMon**, dzięki któremu można oglądać obrazy z kamer na smartfonie, przeglądać zdarzenia, zdalnie włączać i wyłączać wyjścia alarmowe oraz dokonywać zmian w ustawieniach rejestratora. Funkcja *SMART* monitoruje stan i temperaturę dysków, przez co poprawia się niezawodność pracy całego urządzenia. Po wykryciu nieprawidłowej pracy dysków użytkownik jest powiadamiany poprzez e-mail oraz serwer Callback.

Program **HDxViewer** pozwala na zarządzanie wieloma rejestratorami, wyświetlanie obrazów ze 128 kamer oraz stwarza możliwość nagrywania obrazów, także w trybie alarmowym – w formacie AVI. Ciekawą funkcją jest tryb dwumonitorowy, tzw. **Dual Monitor**, w którym na jednym monitorze możemy wyświetlać bieżące obrazy z kamer, a na drugim przeglądać archiwalne nagrania. Prędkość zapisu wynosi 100/200/400 kl./s dla rozdzielczości CIF i 50/100/100 kl./s dla rozdzielczości D1.

Dystrybutorem produktów firmy CNB w Polsce jest firma GDE Polska.

Bezpośr. inf. Paweł Król
GDE Polska

Samsung wprowadza nową wersję aplikacji iPOLiS MOBILE

Jest już dostępna aktualizacja oprogramowania **Samsung iPOLiS MOBILE** dla urządzeń typu smartphone z systemami operacyjnymi iOS i Android. Aplikacja ta umożliwia udoskonaloną współpracę z kamerami i rejestratorami DVR marki Samsung i oferuje nowe opcje podglądu w czasie rzeczywistym oraz odtwarzania obrazu.

Bezpłatne oprogramowanie w wersji 2.0, dostosowane do platform iTunes i Android Market (obecnie Google Play), jest dostępne w Internecie i pozwala użytkownikom zdalnie kontrolować funkcje panoramowania, wychylania i powiększania obrazu z najnowszych kamer sieciowych marki Samsung poprzez prosty, intuicyjny interfejs. Jest także kompatybilne z rejestratorami serii SRD marki Samsung. Po dokonaniu konfiguracji, co zajmuje mniej niż minutę, użytkownicy mogą przeglądać obrazy z wybranych kamer przesłane poprzez bezprzewodową sieć WiFi lub sieć komórkową 3G/4G.

– Oryginalna wersja tej aplikacji zdobyła ogromną popularność wśród klientów, którzy oczekują maksymalnych korzyści wynikających z zainwestowania w system dozoru wizyjnego Samsung – powiedział **Peter Ainsworth**, Senior Product Manager z Samsung Techwin Europe.

Bezpośr. inf. David Solomons
DRS Marketing

Samsung integruje urządzenia IP z oprogramowaniem Mirasys VMS

Kamery sieciowe Samsung zostały zintegrowane z oprogramowaniem zarządzającym firmy Mirasys

Mirasys VMS może równocześnie odbierać zarówno strumienie wizji z kamer IP, jak i sygnały z kamer analogowych. To bazujące na otwartej architekturze i wykorzystujące kompresję H.264 oprogramowanie może zostać uruchomione na setkach serwerów oraz obsługiwać nieograniczoną liczbę stacji roboczych, a także klientów sieci komórkowych lub internetowych.

– *Oferujemy zarazem analogowe, sieciowe i hybrydowe systemy dozoru. Rozumiemy, że klienci muszą mieć możliwość wyboru produktów, które najlepiej odpowiadają ich wymaganiom* – powiedział **Tim Biddulph**, IP Product Manager w **Samsung Techwin Europe**. – *Nasza integracja z Mirasys jest częścią programu integracji z wiodącymi dystrybutorami niezależnego oprogramowania (ISV), którzy mogą zaoferować otwarte aplikacje opracowane specjalnie do łączenia urządzeń i systemów różnych producentów.*

Zespoły inżynierskie firm Mirasys i Samsung podjęły bardzo bliską współpracę, aby zapewnić wysoki poziom integracji, który pozwoli użytkownikom systemu Mirasys sterować wielofunkcyjnymi kamerami sieciowymi marki Samsung. Oprogramowanie stwarza możliwość automatycznego wykrywania kamer, sterowania funkcjami PTZ i dwukierunkowej transmisji dźwięku, sterowania wejściami i wyjściami alarmowymi, korzystania z funkcji detekcji ruchu, włączania i wyłączania promienników IR oraz synchronizacji czasowej, dzięki której serwer może automatycznie zsynchronizować kamery z czasem systemowym.

– *Rozwijamy partnerstwo technologiczne z firmami opracowującymi innowacyjne oprogramowanie, takimi jak Mirasys. Działamy tak zgodnie z naszą filozofią Smart Security. Wyjaśniamy instalatorom, integratorom systemów oraz użytkownikom końcowym, w jaki sposób mogą dobrać urządzenia sieciowe marki Samsung, aby te z nawiązką spełniły ich oczekiwania* – powiedział Tim Biddulph.

– *Zaawansowana integracja kamer sieciowych Samsung z naszymi rozwiązaniami VMS podkreśla naszą bliską współpracę w ramach programu Mirasys Platinum Partner* – powiedział **Jukka Riivari**, dyrektor generalny firmy **Mirasys**. – *Dzięki obsłudze zaawansowanych funkcji kamer, takich jak dwukierunkowa, jednoczesna transmisja dźwięku, detekcja ruchu czy strefy prywatności, nasi wspólni partnerzy handlowi mogą docenić nowe, wyjątkowe możliwości biznesowe, jakie daje połączenie oprogramowania Mirasys z kamerami Samsung.*

Bezpośr. inf. David Solomons
DRS Marketing

Fot. 1. Gary Rowden – dyrektor sprzedaży i marketingu w Samsung Techwin Europe

Samsung
firma nastawiona na sukces

W lutym 2012 na stanowisko dyrektora do spraw sprzedaży i marketingu w firmie Samsung Techwin Europe został powołany Gary Rowden. Było to nowe stanowisko, stworzone w wyniku analizy metod promowania i sprzedaży produktów tej firmy na obszarze Europy. W tym wywiadzie Gary wyjaśnia, w jaki sposób firma realizuje strategię umożliwiającą lepsze zaspokajanie potrzeb klientów, zarówno w dziedzinie sprzedaży jak i obsługi technicznej dostarczanych urządzeń

Redakcja: *Gary, pełnisz swoje nowe obowiązki zaledwie od kilku miesięcy. Czy po upływie tak krótkiego czasu jesteś w stanie powiedzieć coś na temat zasadniczych zmian, jakie są zapowiadane w waszej firmie?*
G. R.: Na szczęście dysponuję bardzo doświadczonym, wysoce profesjonalnym zespołem, który przez ostatnich pięć lat odnosił znaczące sukcesy i moja rola polega na realizacji nowych pomysłów opartych na dotychczasowych osiągnięciach, a nie na wprowadzaniu radykalnych zmian w istniejącej strukturze sprzedaży i obsługi technicznej.

Redakcja: *Które obszary biznesowe mogą być twoim zdaniem usprawnione?*
G. R.: Naszym zasadniczym celem jest umocnienie pozycji firmy Samsung na rynku zabezpieczeń technicznych i stworzenie obrazu firmy, na której można polegać.

Redakcja: *Czy możesz wyjaśnić, co przez to rozumiesz?*
G. R.: Firma Samsung została uznana przez niezależne firmy sondażowe za jednego z czołowych europejskich dostawców sprzętu wykorzystywanego do budowy zabezpieczeń technicznych, jednakże nasza dotychczasowa silna pozycja utożsamiana była z rozwiązaniami analogowymi. Obecnie kładziemy duży nacisk na oferowanie urządzeń sieciowych. Oczywiście to nam nie wystarcza. Chcemy oferować zintegrowane systemy kontroli dostępu oraz dozoru wizyjnego, w których wykorzystujemy rozwiązania specyficzne dla marki Samsung, traktowane jako najlepsze w swojej klasie. Ponadto, w oparciu o naszą sieć dystrybucyjną, pragniemy zdyskontować tę wysoką pozycję i zapewnić naszym odbiorcom usługi serwisowe i wsparcie techniczne.

Redakcja: *Czy uważasz, że dotychczas firma Samsung oferowała wsparcie techniczne i usługi serwisowe na poziomie satysfakcjonującym waszych klientów?*
G. R.: Zdecydowanie tak. Z informacji otrzymywanych z rynku wynika, że w znakomitej większości przypadków klienci byli zadowoleni z naszych wysiłków marketingowych, ułatwiających im odnoszenie sukcesów w działalności biznesowej, a także z działań prowadzonych przez nasze ekipy techniczne. Bez wątpienia oferowane przez nas darmowe usługi projektowe oraz darmowa obsługa serwisowa zostały wysoko ocenione przez klientów. Nie bez znaczenia była trzyletnia gwarancja, potwierdzająca naszą wiarygodność rynkową oraz niezawodność i trwałość naszych produktów.

Aby zyskać zaufanie, należy jednak krytycznie oceniać własne działania. Ciągle dążymy do ulepszania naszych produktów. Z tego powodu staliśmy się „ofiarami" własnego sukcesu.

Redakcja: *Co przez to rozumiesz?*
G. R.: Mówiąc prościej, wzrost sprzedaży, jaki odnotowaliśmy w ostatnich kilku latach, przekroczył nasze najśmielsze oczekiwania i spowodował, że tak samo wzrosły wymagania klientów związane z obsługą marketingową i techniczną. Zaproponowanie darmowego wsparcia technicznego stanowi doskonały sposób na zyskanie zaufania klientów, jednak zmusza do zgromadzenia odpowiednich środków do jego realizacji.

Redakcja: *Czy nie utrudni to przyszłej działalności firmy Samsung?*
G. R.: Jesteśmy zdeterminowani, by tak się nie stało. Reagujemy na wyzwania rzucane przez rynek i w naszej głównej siedzibie zatrudniamy dodatkowy, doświadczony personel techniczny.

Oczywiście równie istotne jest zatrudnienie personelu pracującego w terenie, na poziomie lokalnym, mówiącego wspólnym językiem i rozumiejącego potrzeby występujące na lokalnych rynkach. Z tego powodu już teraz inwestujemy w personel zatrudniany w naszych oddziałach we Francji, Włoszech, w Niemczech, Czechach, Hiszpanii i w Rosji, jak również w siedzibie głównej w Wielkiej Brytanii. Nasze produkty pochodzą z Korei, jednak w przyszłości firma Samsung Techwin Europe będzie zarządzana przez lokalnych menadżerów, którzy będą lepiej rozumieć i spełniać wymagania klientów na poziomie lokalnym.

Oprócz rekrutacji wartościowych pracowników prowadzimy również inne działania zmierzające do utwierdzenia nowych i dotychczasowych klientów w przekonaniu, że mogą oni łatwo uzyskać wszystkie niezbędne informacje. Wkrótce uruchomimy nową, wielojęzyczną stronę internetową, przeznaczoną dla klientów europejskich, na której instalatorzy, integratorzy systemów, projektanci oraz użytkownicy końcowi będą mieli dostęp do czytelnych informacji dotyczących całego asortymentu produktów oferowanych przez firmę Samsung, dzięki czemu będą mogli wybrać odpowiedni zestaw produktów oraz zapoznać się z możliwościami ich wzajemnego połączenia.

Redakcja: *Co przyniesie przyszłość działowi zabezpieczeń profesjonalnych firmy Samsung?*
G. R.: Na terenie całej Europy mamy stałych klientów. Już teraz otaczamy ich stałą opieką i mamy zamiar uczynić wszystko, co jest konieczne, by umocnić ich lojalność i zaufanie, dlatego widzimy przyszłość w jasnych barwach. Stawiamy na nasze produkty sieciowe. Dotychczas sieciowe systemy dozorowe były postrzegane jako przydatne podczas realizacji dużych projektów, jednakże obecnie odnotowujemy coraz częstsze przypadki stosowania ich w małych i średnich instalacjach. Ta tendencja zaczyna znajdować uzasadnienie ekonomiczne.

Fot. 2. Rozwiązania sieciowe firmy Samsung

By stworzyć ułatwienia dla klientów chcących stopniowo zastąpić systemy analogowe rozwiązaniami w pełni wykorzystującymi sieci IP, przyspieszamy realizację naszego programu integracji kamer firmy Samsung i rejestratorów typu DVR i NVR z oferowanym przez niezależnych producentów oprogramowaniem służącym do zarządzania systemami dozorowymi. Daje to nowe możliwości naszym klientom, gdyż wyroby firmy Samsung mogą być stosowane wraz z produktami innych producentów. Firmy Axxon, Aimetis, Digifort, Griffid, Ipronet, Exacq, Genetec, ISS, Milestone, Mirasys, ONssi i Seetec to tylko niektórzy spośród producentów oprogramowania VMS wykorzystywanego przez takie firmy jak nasza. Ich produkty należą do klasy „otwartej" i mogą być łatwo adaptowane.

Redakcja: *Czy myślisz, że większość instalatorów ma wiedzę dotyczącą sieciowych systemów dozorowych?*
G. R.: Poza liczną rzeszą instalatorów i integratorów systemów, którzy mają odpowiednią wiedzę na temat sieciowych systemów dozorowych, jest równie liczna lub nawet większa grupa instalatorów, którzy nawet nie wiedzą, jakie pytania trzeba zadać, gdy wymaga się od nich skompletowania sprzętu niezbędnego do utworzenia rozwiązania sieciowego. Jako reprezentanci przemysłu związanego z systemami zabezpieczającymi uważamy, że bardzo istotne jest dzielenie się naszą wiedzą i doświadczeniem z naszymi obecnymi i potencjalnymi klientami. Nasza filozofia *Smart Security* stanowi w istocie wszystko to, co nasi klienci z naszą pomocą mogą zyskać, stopniowo zastępując systemy analogowe sieciowymi. W najbliższych miesiącach będziemy organizować kursy szkoleniowe, podczas których instalatorzy i integratorzy systemów dowiedzą się, jak rekomendować sieciowe rozwiązania firmy Samsung, oraz utwierdzą się w przekonaniu, że rozwiązania te spełnią, a nawet przewyższą oczekiwania użytkowników końcowych. Chcemy także odczarować instalacje i rozwiązania sieciowe, pozbawić je tajemniczości. Wykażemy, że dzięki naszemu doradztwu i wsparciu klienci nie powinni obawiać się stosowania nowatorskich technologii oferujących tak liczne korzyści. Jedną z takich korzyści jest możliwość zastosowania kamer megapikselowych, w tym najnowszych kamer o rozdzielczości HD.

Redakcja: *Czy myślisz, że instalatorzy mogą mieć problemy z powodu wprowadzenia przez firmę Samsung na rynek tak wielu nowych produktów i technologii w relatywnie krótkim czasie?*
G. R.: Większość nowych technologii wprowadzanych na rynek systemów zabezpieczeń ma swoje korzenie w inwestycjach poczynionych przez firmy podobne do Samsunga, prowadzących do rozwoju produktów przeznaczonych na rynek konsumencki. Postęp technologiczny stanowi odpowiedź na rosnące wymagania użytkowników końcowych. Niezależnie od przyczyn, tempo z jakim wprowadzane są nowe technologie nie stanowi zasadniczego problemu. Problemy, z jakimi mamy do czynienia, wynikają jedynie z braku odpowiedniego przeszkolenia i wiedzy dotyczącej sposobów zastosowania nowych technologii, a także z niezrozumienia korzyści, jakie wynikają z nadchodzących zmian. Szkolenia są bardzo ważne. Wkrótce nasi klienci będą zapraszani do wzięcia udziału w programach edukacyjnych oferowanych przez nowo utworzoną placówkę Samsung IP Institute (SIPI).

www.dmaxpolska.pl

nadchodzi nowy

NAJWAŻENIEJSZE CECHY

- **F-DNR (Defog)** - niweluje zakłócenia (mgła, opady śniegu)
- **COAXIAL** – sterowanie po kablu koncentrycznym
- **WDR** – szeroki zakres dynamiki
- **DIS** – cyfrowa stabilizacja obrazu
- **Smart D-zoom** – inteligentny cyfrowy zoom
- **650 TVL** kolor

D-max POLSKA

Ochrona systemów nadzoru wizyjnego CCTV przed przepięciami

Tomasz Maksimowicz

Systemy telewizji dozorowej są wykorzystywane do nadzoru prowadzonego w celu zwiększenia bezpieczeństwa obszarów mieszczących się zarówno wewnątrz, jak i na zewnątrz budynków. W celu ochrony systemów CCTV przed uszkodzeniami i zapewnienia ich niezawodności powinno się zabezpieczać je przed oddziaływaniem wyładowań atmosferycznych, które zakłócają ich funkcjonowanie. Szkody wywołane przez bezpośrednie lub pośrednie (przepięcia indukowane) oddziaływanie prądu pioruna mogą skutkować nie tylko poważnymi stratami finansowymi związanymi z fizycznym uszkodzeniem sprzętu, ale przede wszystkim z utratą funkcjonalności systemu, która zmniejsza bezpieczeństwo obiektu

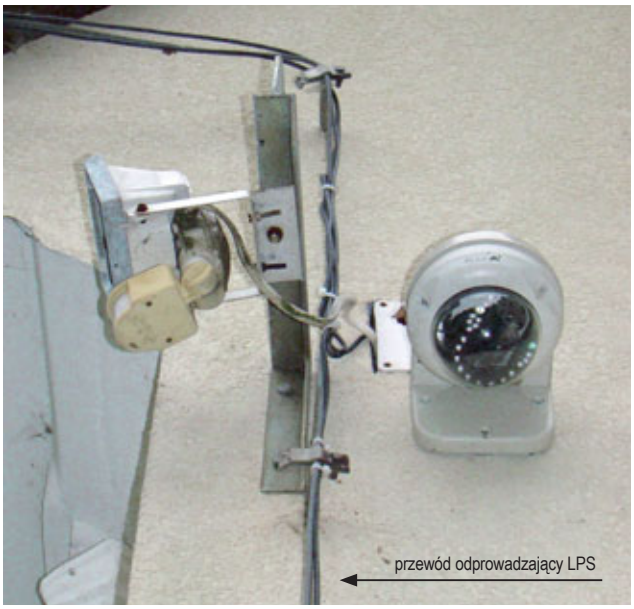
Źródła zagrożeń

Istnieje wiele dróg, którymi przedostają się przepięcia stanowiące zagrożenie dla poszczególnych podzespołów systemu CCTV, w skład którego wchodzą urządzenia zainstalowane w centrum nadzoru wizyjnego oraz punkty kamerowe rozmieszczone często na rozległych obszarach.

Kamery umieszczane na zewnętrznej konstrukcji budynków lub na słupach w terenie otwartym narażone są na bezpośrednie oddziaływanie prądu piorunowego. Energia, jaką niesie impuls pioruna, może nie tylko spowodować zniszczenie sprzętu znajdującego się na zewnątrz budynku, ale także przeniknąć poprzez linie zasilające i sygnałowe do jego wnętrza, powodując jeszcze poważniejsze straty w centrum nadzoru wizyjnego. O ile uszkodzenie pojedynczej kamery powoduje jedynie częściową utratę funkcjonalności, awaria urządzeń w centrum systemu może całkowicie przerwać jego funkcjonowanie i spowodować utratę ważnych danych. W związku z tym wszelkie elementy zewnętrzne systemu powinny znajdować się w strefie ochronnej instalacji odgromowej (LPS, ang. *lightning protection system*) zgodnie z obowiązującymi normami serii PN-EN 62305 [1].

Istotne źródło zagrożenia stanowią przepięcia pochodzące z zewnętrznych linii zasilających obiekt. Przy bezpośrednim uderzeniu pioruna w linię energetyczną prąd piorunowy zagraża wszystkim podzespołom wymagającym zasilania, o ile nie są one odpowiednio zabezpieczone. Ze względu na znaczne długości tras kablowych stosowanych w instalacjach CCTV zagrożeniem dla systemu są także przepięcia indukowane. W tym przypadku zagrożone są nie tylko połączenia z punktami kamerowymi na zewnątrz budynku, ale także w jego wnętrzu. Na przepięcia narażone są zarówno linie zasilające (AC lub DC), jak i kable sygnałowe (tory wizji i sterowania kamer). W normach PN-EN 50130-4 określone są wymagania dotyczące poziomów odporności urządzeń stosowanych w systemach alarmowych [2]. Zarówno wartości szczytowe udarów wytwarzanych podczas badań kompatybilności urządzeń alarmowych (maksymalnie do 2 kV udar 1,2/50 μs) oraz maksymalne wartości napięć, jakie są w stanie wytrzymać te urządzenia są znacznie mniejsze od wartości przepięć, jakie mogą pojawić się w okablowaniu wskutek wyładowań atmosferycznych, w związku z czym konieczne jest stosowanie środków ochrony przed przepięciami.

Niestety w praktyce sami projektanci i wykonawcy systemów CCTV zwiększają zagrożenie systemu i życia ludzkiego poprzez złe rozmieszczanie punktów kamerowych i błędne prowadzenie tras kablowych. Wynika to przede wszystkim z braku podstawowej wiedzy z zakresu ochrony odgromowej. W przypadku instalowania podzespołów systemu CCTV w istniejących budynkach rzadko zwraca się uwagę na zachowanie bezpiecznych odstępów izolacyjnych pomiędzy kamerami a zwodami lub innymi przewodami odprowadzającymi należącymi do instalacji odgromowych. Przykłady często popełnianych błędów montażowych przedstawiono na rysunku 1. W przypadku bezpośredniego uderzenia pioruna w budynek, przy przepływie prądu piorunowego przez przewody instalacji odgromowej, może nastąpić przeskok iskry do umieszczonych zbyt blisko instalacji



Rys. 1. Błędy przy montażu kamer systemu CCTV: niezachowanie bezpiecznych odstępów izolacyjnych i prowadzenie kabli wzdłuż przewodu odprowadzającego instalacji odgromowej

(kamer lub przewodów). Prowadzenie kabli wzdłuż przewodów odprowadzających prąd piorunowy stwarza możliwość częściowego przeniku tego prądu do wewnętrznych instalacji systemu alarmowego. Może to poskutkować zniszczeniem urządzeń elektronicznych i porażeniem istot żywych.

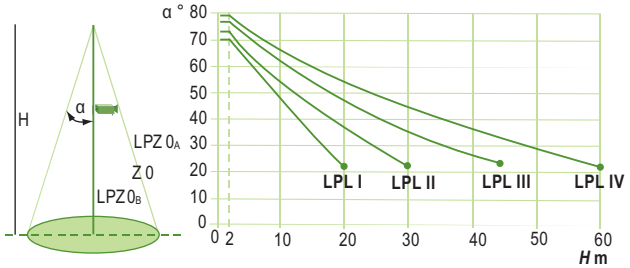
Ochrona odgromowa

Koncepcja ochrony przedstawiona w serii norm PN-EN 62305 zakłada podział obiektu na strefy ochrony odgromowej (LPZ, ang. *lightning protection zone*), które można zdefiniować następująco:

- **LPZ 0_A** – strefa na zewnątrz budynku, w której występuje zagrożenie wyładowania bezpośredniego oraz oddziaływanie całkowitego prądu pioruna i całkowitego pola magnetycznego;
- **LPZ 0_B** – strefa na zewnątrz budynku, w której nie występuje zagrożenie wyładowania bezpośredniego, ale możliwe jest oddziaływanie częściowego prądu pioruna lub prądów indukowanych oraz całkowitego pola magnetycznego;
- **LPZ 1…N** – strefy wewnątrz obiektu, w których nie występuje zagrożenie wyładowania bezpośredniego, ale możliwe jest oddziaływanie ograniczonego prądu pioruna lub prądów indukowanych oraz całkowitego lub stłumionego pola magnetycznego.

Typ 1	chroniące przed bezpośrednim oddziaływaniem prądu pioruna, badane prądem udarowym o kształcie 10/350 μs, stosowane w rozdzielnicach głównych
Typ 2	chroniące przed przepięciami indukowanymi i napięciami „resztkowymi" z ograniczników typu 1, badane prądem udarowym o kształcie 8/20 μs, stosowane w rozdzielnicach lokalnych
Typ 3	chroniące przed przepięciami indukowanymi, badane prądem udarowym o kształcie 8/20 μs, charakteryzujące się niskimi poziomami napięć ochronnych, stosowane w rozdzielnicach lokalnych lub bezpośrednio przy urządzeniach

Tab. 1. Typy ograniczników przepięć dla sieci rozdzielczych niskiego napięcia



Rys. 2. Zależność kąta osłonowego α od wysokości H zwodu pionowego względem płaszczyzny odniesienia i poziomu ochrony odgromowej LPL

Wszystkie kamery umieszczane na zewnętrznych ścianach lub dachu budynku oraz na słupach kamerowych powinny znajdować się w strefie LPZ 0_B tworzonej przez konstrukcję budynku lub układ zwodów pionowych i poziomych instalacji odgromowej. Strefę 0_B wyznacza się metodą wirtualnej kuli toczonej po powierzchni obiektu (metoda bardziej dokładna) lub na podstawie kąta osłonowego α w przypadku zwodów pionowych. W części trzeciej serii norm PN-EN 62305 zdefiniowano cztery klasy LPS odpowiadające poszczególnym poziomom ochrony odgromowej (LPL ang. *lightning protection level*). Dla każdej z klas zdefiniowano między innymi wymagania dotyczące minimalnych odstępów między zwodami i przewodami odprowadzającymi instalacji odgromowej, promienia toczonej kuli r oraz wartości kątów osłonowych α dla zwodów pionowych (rys. 2).

Kamery umieszczane na słupach także powinny znajdować się w strefie osłonowej tworzonej przez zwody pionowe. Zwody te powinny być połączone z uziomem obiektu.

Przy projektowaniu rozmieszczenia kamer i tras kabli na budynku należy uwzględnić możliwość przeskoków iskrowych z elementów LPS przewodzących prąd pioruna. Wszelkie instalacje powinny znajdować się w bezpiecznych odstępach izolacyjnych od zwodów i przewodów odprowadzających, które nie powinny być mniejsze niż:

$$s = \frac{k_i}{k_m} \times k_c \times l$$

gdzie:

k_i – współczynnik zależny od wybranej klasy LPS: 0,08, 0,06 lub 0,04 odpowiednio dla LPS klasy I, II lub III i IV,

k_m – współczynnik zależny od materiału izolacyjnego, przyjmujący wartość 1 dla powietrza lub 0,5 dla betonu, cegieł lub drewna,

k_c – współczynnik zależny od rozpływu prądu w elementach LPS,

l – długość (w metrach) mierzona wzdłuż przewodu LPS od miejsca instalacji kamery do punktu najbliższego połączenia wyrównawczego LPS.

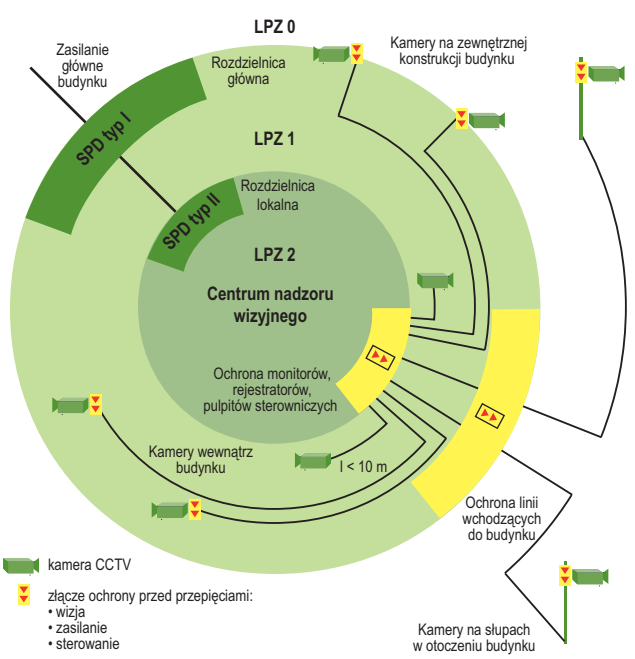
W pierwszej edycji norm PN-EN 62305 (przywołanej w Rozporządzeniu Ministra Infrastruktury) wartość współczynnika k_c była wyznaczana w zależności od liczby przewodów odprowadzających oraz od typu uziemienia (uziom poziomy/pionowy typu A lub uziom otokowy typu B). W drugiej edycji norm przedstawiono natomiast metodę uproszczoną oraz metodę dokładną. Metoda uproszczona zakłada wartości k_c równe 1, 0,66 lub 0,44 (w zależności od liczby przewodów odprowadzających) odpowiednio dla 1, 2 lub 3 i większej liczby przewodów. Metoda dokładna pozwala na oszacowanie, czy możliwe są mniejsze odstępy s, jednak wymaga głębszej analizy rozpływu prądu pioruna w instalacji LPS. W niektórych przypadkach możliwe jest także wybranie wartości k_c na podstawie przedstawionych w normie przykładów.

Ochrona przed przepięciami

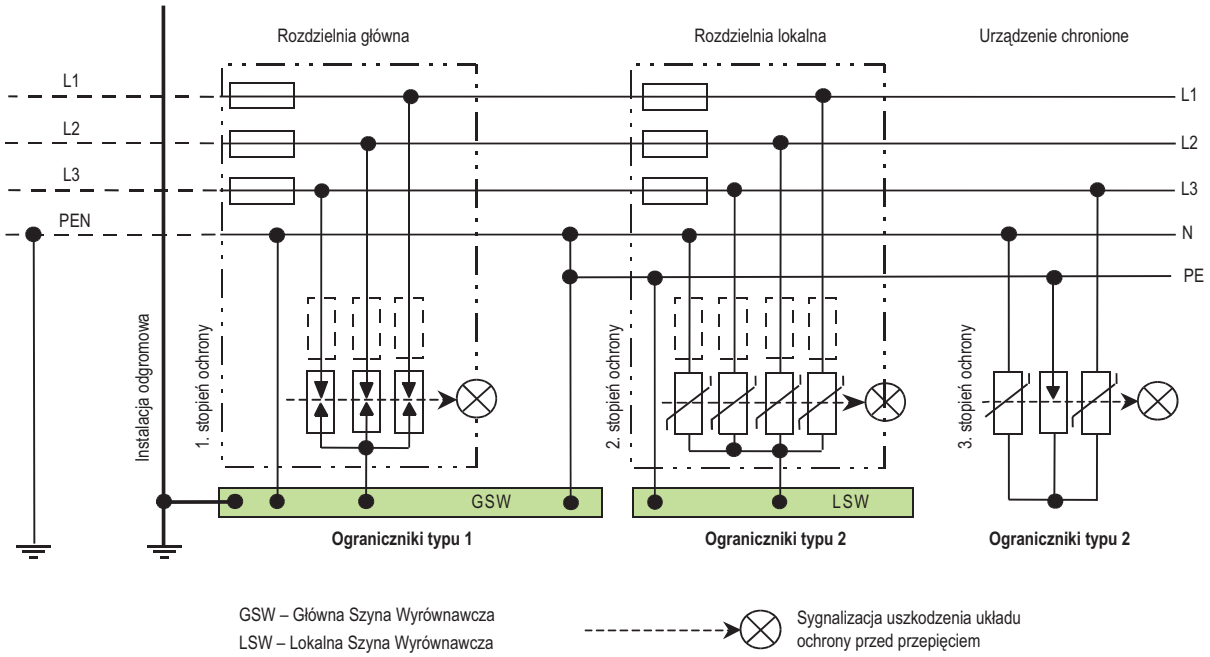
Ochrona przed przepięciami powinna być projektowana zgodnie ze strefową koncepcją ochrony opisaną w serii norm PN-EN 62305. Poza opisanymi wcześniej strefami zewnętrznymi LPZ 0_A i LPZ 0_B w ogólnym przypadku analizy systemów CCTV można zdefiniować także dwie strefy wewnętrzne:

– LPZ 1 – wnętrze budynku,
– LPZ 2 – pomieszczenie centrum nadzoru wizyjnego (LPZ 2 znajduje się wewnątrz LPZ 1).

W przypadku niewielkich budynków może nie być potrzeby określania strefy LPZ 2. Strefowa koncepcja ochrony zakłada stosowanie układów do ograniczania przepięć na granicach poszczególnych stref. Chronione powinny być wszelkie linie zasilające oraz sygnałowe, do których zalicza się tory służące do transmisji sygnałów wizyjnych i sterujących, prowadzących do kamer. Wewnątrz budynku układy ochronne powinny być stosowane na wejściu wszystkich linii wprowadzanych do pomieszczenia centrum nadzoru wizyjnego (granica LPZ 1/2), co pozwala na zabezpieczenie znajdujących się tam urządzeń, do których można zaliczyć monitory, rejestratory, krosownice czy pulpity sterownicze. Poszczególne punkty kamerowe znajdujące się wewnątrz budynku wymagają także dodatkowego zabezpieczenia, gdy długość tras kablowych od strefy LPZ 2 jest większa niż kilkanaście metrów, ze względu na możliwość występowania przepięć indukowanych. Kamery umieszczane na zewnętrznej konstrukcji budynku i słupach także wymagają zabezpieczenia. W przypadku, gdy kamera



Rys. 3. Koncepcja strefowej ochrony systemu CCTV przed przepięciami



Rys. 4. Przykład stosowania ograniczników różnego typu w sieci zasilającej typu TN-C-S

jest umieszczana na ścianie budynku, wszelkie linie zasilające i sygnałowe powinny być wprowadzone do wnętrza jak najkrótszą drogą. Linie z kamer znajdujących się w terenie zaleca się wprowadzać do budynku i zabezpieczać w jednym punkcie (granica LPZ 0/1). Koncepcja strefowej ochrony systemu CCTV przed przepięciami została przedstawiona na rysunku 3.

Ochrona przeciwprzepięciowa linii zasilającej

Ograniczniki przepięć stosowane w liniach zasilających powinny spełniać wymagania zawarte w PN-EN 61643-11 [5], gdzie opisano metody badań takich układów. Zdefiniowano trzy typy ograniczników opisane w tabeli 1.

Ochrona od strony zasilania energetycznego powinna być zapewniona już w rozdzielnicy głównej na wejściu linii zasilającej do budynku (granica stref LPZ 0_A/1). Należy stosować tam ograniczniki typu 1. Obecnie tylko renomowani producenci oferują iskiernikowe ograniczniki przepięć wykonywane w technologii bezwydmuchowej, zdolne do odprowadzenia prądu piorunowego o wartości szczytowej nawet do 100 kA impulsu 10/350 μs. Ograniczniki typu 1 zapewniają zazwyczaj poziom ochrony poniżej 4 kV lub 2,5 kV, dlatego niezbędne jest zapewnienie drugiego stopnia ochrony przez zastosowanie ograniczników typu 2 w rozdzielnicy lokalnej zasilającej centrum nadzoru wizyjnego (granica stref LPZ 1/2). Ograniczniki przepięć w rozdzielnicy lokalnej powinny sprawić, że wartość szczytowa udarów będzie niższa od maksymalnych wartości napięć wytrzymywanych przez znajdujące się tam urządzenia.

Dopuszcza się także stosowanie ograniczników kombinowanych typu 1 + 2, zdolnych do odprowadzenia prądu piorunowego i ograniczających napięcia do niższych poziomów (rys. 5).

Jeżeli długość linii zasilającej pomiędzy urządzeniem znajdującym się w centrum nadzoru a rozdzielnicą lokalną lub pomiędzy punktem kamerowym a przyłączem energetycznym jest większa niż kilkanaście metrów, to bezpośrednio przy urządzeniu końcowym należy zastosować ograniczniki przepięć typu 3 w celu ochrony przed przepięciami indukowanymi. Ograniczniki przepięć należy dobierać odpowiednio do znamionowego napięcia zasilania kamer – najczęściej jest to napięcie przemienne 230 V lub 24 V, lub napięcie stałe 12 V. Jeżeli napięcie zasilające jest niższe niż 230 V często, bezpośrednio przy kamerach, stosowane są przetwornice. W takim przypadku ochrona przed przepięciami powinna być zastosowana na wejściu do przetwornicy.

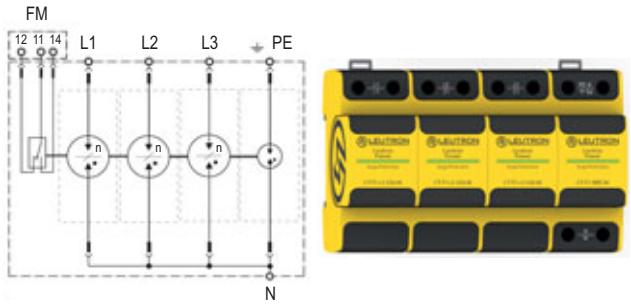
Ochrona przeciwprzepięciowa torów sygnałowych

Ograniczniki przepięć stosowane do ochrony linii sygnałowych powinny spełniać wymagania normy PN-EN 61643-21. W kartach katalogowych można spotkać się z oznaczeniami kategorii C1, C2, C3, D1 lub D2.

Kategorie te definiują poziomy udarów, na jakie narażony jest dany typ ogranicznika podczas badań, a tym samym określają jego odporność udarową. Obecnie większość ukła-

Kat.	Typ próby	Napięcie obwodu otwartego	Prąd obwodu zwartego	Minimalna liczba udarów
C1	Szybki czas narastania	0,5 kV lub 1 kV, 1,2/50 μs	0,25 kA lub 0,5 kA, 8/20 μs	300
C2		2 kV, 4 kV lub 10 kV, 1,2/50 μs	1 kA, 2 kA lub 5 kA, 8/20 μs	10
C3		$\geq$ 1 kV, 1 kV/μs	10 A, 25 A lub 100 A, 10/1000 μs	300
D1	Duża energia	$\geq$ 1 kV	0,5 kA, 1 kA lub 2,5 kA, 10/350 μs	2
D2		$\geq$ 1 kV	1 kA lub 2,5 kA, 10/250 μs	5

Tab. 2. Parametry udarów prądowych i napięciowych stosowanych w badaniach ograniczników przepięć dla linii sygnałowych

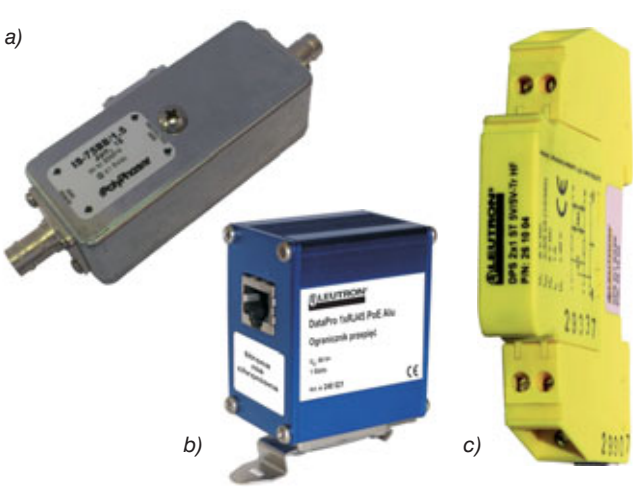


Rys. 5. Układ ogranicznika Leutron typu CT-T1+2/3+1-350-FM (ogranicznik typu 1 + 2) do zabezpieczenia rozdzielni głównej

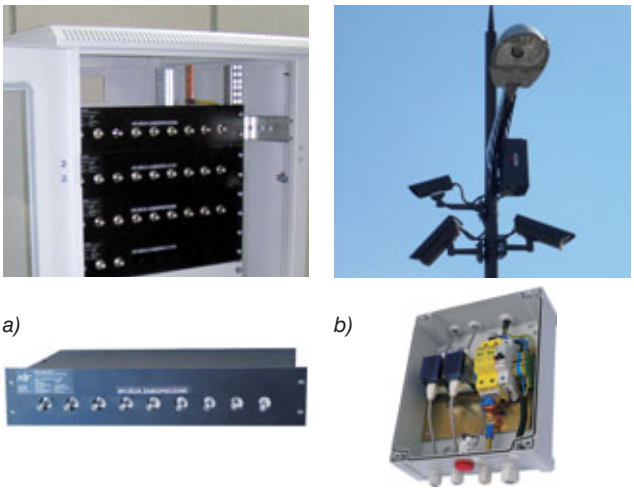
dów ograniczających przepięcia należy do kategorii C1/C2/C3. Ograniczniki kategorii D1 charakteryzują się wyższym poziomem odporności i nawet są w stanie odprowadzić część prądu pioruna. Poszczególne kategorie scharakteryzowano w tabeli 2.

W systemach CCTV do transmisji sygnału wizji oraz sygnałów służących do sterowania kamerami wykorzystywane są najczęściej popularne złącza, takie jak BNC, RJ45, RS485 czy RS422. Ograniczniki przepięć powinny być dobierane z uwzględnieniem napięć znamionowych i zakresów częstotliwości sygnałów stosowanych w danym systemie. Napięciowy poziom ochrony ogranicznika powinien być mniejszy niż maksymalne napięcie wytrzymywane przez chronione urządzenie. Przykłady ograniczników przepięć dla linii sygnałowych przedstawiono na rysunku 6.

Obecnie dostępnych jest wiele rozwiązań przeznaczonych do ochrony systemów CCTV przed przepięciami. Na rysunku 6a przedstawiono układ do ochrony maksymalnie dziewięciu koncentrycznych torów wizyjnych umożliwiający skuteczne zabezpieczenie multipleksera lub rejestratorów w centrum nadzoru wizyjnego. Z kolei rysunek 6b przedstawia układ do kompleksowego zabezpieczenia punktu kamerowego umieszczonego w jednej obudowie, chroniącego przed przepięciami tor wizyjny, tor sterujący oraz obwód zasilania kamery. Takie rozwiązanie może być stosowane bezpośrednio przy kamerze umieszczonej na ścianie na zewnątrz budynku lub na słupie kamerowym.



Rys. 6. Przykłady ograniczników przepięć linii sygnałowych różnych standardów: a) linia koncentryczna; b) sieć LAN; c) para żył



Rys. 7. Dedykowane układy do ochrony systemów CCTV: a) ochrona torów sygnałowych centrum dozoru wizyjnego; b) złącze do ochrony punktu kamerowego przed przepięciami

Podsumowanie

Ochrona odgromowa i przed przepięciami, która jest zgodna z obowiązującymi normami, pozwala uniknąć strat materialnych oraz zwiększa niezawodność systemów nadzoru wizyjnego CCTV. Należy zwracać szczególną uwagę na rozmieszczenie punktów kamerowych i prowadzenie tras kablowych w odpowiedniej odległości od przewodów LPS. Układy ograniczników przepięć powinny być stosowane nie tylko do ochrony poszczególnych punktów kamerowych, ale także do zabezpieczenia centrum nadzoru wizyjnego.

Opracowanie: dr inż. Tomasz Maksimowicz
RST sp. j., ul. Myśliwska 2, 15-569 Białystok
e-mail: rst@rst.pl, www.rst.pl

Bibliografia

1. PN-EN 62305-1 *Ochrona odgromowa – Część 1: Zasady ogólne.*
2. PN-EN 62305-3 *Ochrona odgromowa – Część 3: Uszkodzenia fizyczne obiektów i zagrożenie życia.*
3. PN-EN 62305-4 *Ochrona odgromowa – Część 4: Urządzenia elektryczne i elektroniczne w obiektach.*
4. PN-EN 50130-4 *Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów sygnalizacji pożarowej, sygnalizacji włamania, sygnalizacji napadu, CCTV, kontroli dostępu i osobistych.*
5. PN-EN 61643-11 *Niskonapięciowe urządzenia do ograniczania przepięć – Część 11: Urządzenia do ograniczania przepięć w sieciach rozdzielczych niskiego napięcia – Wymagania i próby.*
6. PN-EN 61643-21 *Niskonapięciowe urządzenia ograniczające przepięcia – Część 21: Urządzenia do ograniczania przepięć w sieciach telekomunikacyjnych i sygnalizacyjnych – Wymagania eksploatacyjne i metody badań.*

Pełny obraz sytuacji

Uchwyć szczegóły kamerą
Dinion 1080p HD firmy Bosch

ZŁOTY MEDAL ETP 2012

Bosch Dinion 1080p HD zapewnia bardzo wysoką rozdzielczość obrazu, doskonałą pracę nawet w warunkach słabego oświetlenia sceny oraz niezrównaną reprodukcję kolorów. Dzięki inteligentnej analizie obrazu żadne zagrożenie nie umknie Twojej uwadze!

Sprawdź pełną ofertę rozwiązań HD fi rmy Bosch na **www.boschsecurity.pl**

BOSCH
Technologia bliżej nas

Dinion NBN-832 HD

nowa kamera firmy Bosch

Michał Biela

Firma Bosch tworzy coraz doskonalsze produkty, między innymi coraz lepsze kamery. Przykładem może być kamera full HD Dinion NBN-832 (1080p). Jej zaprojektowana od podstaw nowoczesna konstrukcja zapewnia doskonałe działanie. Nowe rozwiązanie pozwala na lepsze odprowadzanie ciepła, co sprawia, że nie są potrzebne dodatkowe elementy chłodzące w celu utrzymania stabilnego, niezawodnego działania w skrajnych warunkach temperaturowych. W kamerze zastosowano nowy układ procesora sygnałowego, dzięki czemu przetwarzanie obrazów stało się szybsze i bardziej efektywne. Urządzenie jest wyposażone w najnowsze oprogramowanie pozwalające maksymalnie wykorzystać możliwości układów elektronicznych. Zastosowanie przetwornika CMOS 1/2,7" HD ze skanowaniem progresywnym, zaprojektowanego w całości przez firmę Bosch, poprawiło reprodukcję barw, a przede wszystkim odwzorowanie scen dynamicznych. Obróbka sygnału wizyjnego powoduje, że sygnał o jakości HD przesyłany jest bez strat. Kamera bardzo dobrze reaguje na szybko zmieniające się oświetlenie, redukując szumy w zacienionych miejscach do minimum.

Kamera Dinion NBN-832 HD została zaprojektowana do strumieniowego przesyłania sygnału wizyjnego o rozdzielczości 1080p w formacie 16:9. Dzięki nowemu oprogramowaniu można uzyskać cztery strumienie wizyjne, w tym trzy H.264 oraz jeden M-JPEG. Umożliwia to swobodne zarządzanie sygnałem wizyjnym.

Korzyści z tej metody to między innymi optymalne wykorzystanie pasma sieciowego i swoboda integracji z systemami zarządzania innych producentów. Kamera jest zgodna ze specyfikacją normy ONVIF (*Open Network Video Interface Forum*), która gwarantuje poprawność działania urządzeń wizyjnych różnych producentów.

Kamery Dinion NBN-832 HD dają wiele możliwości zapisu. Nie trzeba stosować dodatkowego oprogramowania. Wystarczy podłączyć kamerę do sieci IP, a strumień wizyjny będzie zapisywany na urządzeniu typu iSCSI lub bezpośrednio na karcie pamięci microSD o maksymalnej pojemności do 2 TB. Dzięki karcie microSD można podwyższyć poziom bezpieczeństwa i niezawodności zapisu. Włączenie funkcji automatycznego uzupełnienia zapisu ANR w przypadku utraty połączenia sieciowego pomiędzy kamerą a urządzeniem zapisującym iSCSI powoduje, że strumień wizyjny jest zapisywany lokalnie, a po przywróceniu połączenia, nagrania z karty pamięci są automatycznie przenoszone na sieciowe macierze dyskowe iSCSI. Szereg dodatkowych funkcji można uzyskać, korzystając z programu Bosch Video Recording Manager (VRM).

Kamera posiada dwa algorytmy analizy obrazu, podstawowy Motion+ lub rozszerzony z inteligentną analizą obrazu (IVA), ułatwiający monitorowanie scen. Wbudowany dedykowany układ analityczny pozwala na wykrycie obiektu nieruchomego, przekroczenia linii, pojawienia się obiektu w polu widzenia kamery, obiektu o określonej kolorystyce, przekroczenia wirtualnego ogrodzenia, usunięcie obiektu z pola widzenia kamery, zliczania osób itp. Dostępna jest także funkcja inteligentnego wyszukiwania zdarzeń w materiale archiwalnym (*forenscic search*). Operator może w kilka sekund odszukać dane zdarzenie alarmowe w materiale archiwalnym, nawet jeżeli wcześniej go nie zdefiniował. Obie te funkcje opierają się na wykorzystaniu tak zwanych metadanych, które są zapisywane równolegle z sygnałem wizyjnym.

Kamera została zaprojektowana w taki sposób, aby użytkownik, w zależności od potrzeb, mógł wybrać sposób prezentacji sygnału wizyjnego z kamery. W tym celu można skorzystać z przeglądarki internetowej, oprogramowania Bosch Video Management System lub darmowego programu Bosch Video Client, które jest dołączane bezpłatnie do każdej kamery.

Aby ułatwić instalację w urządzeniu dostępne są trzy opcje zasilania – przez przewód sygnałowy (PoE) bądź konwencjonalnie (12 V_{DC}, 24V_{AC}). Interfejs sieciowy wyposażono w funkcję AUTO-MDIX, dzięki czemu nie trzeba pamiętać o używaniu dedykowanych kabli ze skrosowanymi przewodami. Urządzenie samo wykrywa rodzaj użytego kabla.

Automatyczna regulacja ogniskowania (automatyczne ustawienie ostrości) w modelu Dinion NBN-832 HD pozwala na precyzyjne ustawienie ostrości zarówno w dziennym i nocnym trybie pracy. Skraca ona również czas instalacji – nawet o 50%.

Kamera jest wyposażona w przyjazny dla użytkownika interfejs operatora. Za pośrednictwem przeglądarki internetowej można skonfigurować wszystkie funkcje kamery, łącznie z funkcją asystenta automatycznego ogniskowania wybranej strefy i wyborem rodzaju zdarzeń alarmowych analizowanych za pomocą IVA, a także odtworzyć materiał archiwalny.

Urządzenia firmy Bosch są projektowane w taki sposób, aby po opublikowaniu nowej wersji dostosowanego do nich oprogramowania użytkownik mógł sam bezpłatnie dokonać aktualizacji.

Michał Biela
Bosch Security Systems

Kompleksowe układy chroniące systemy CCTV przed przepięciami

Tomasz Maksimowicz

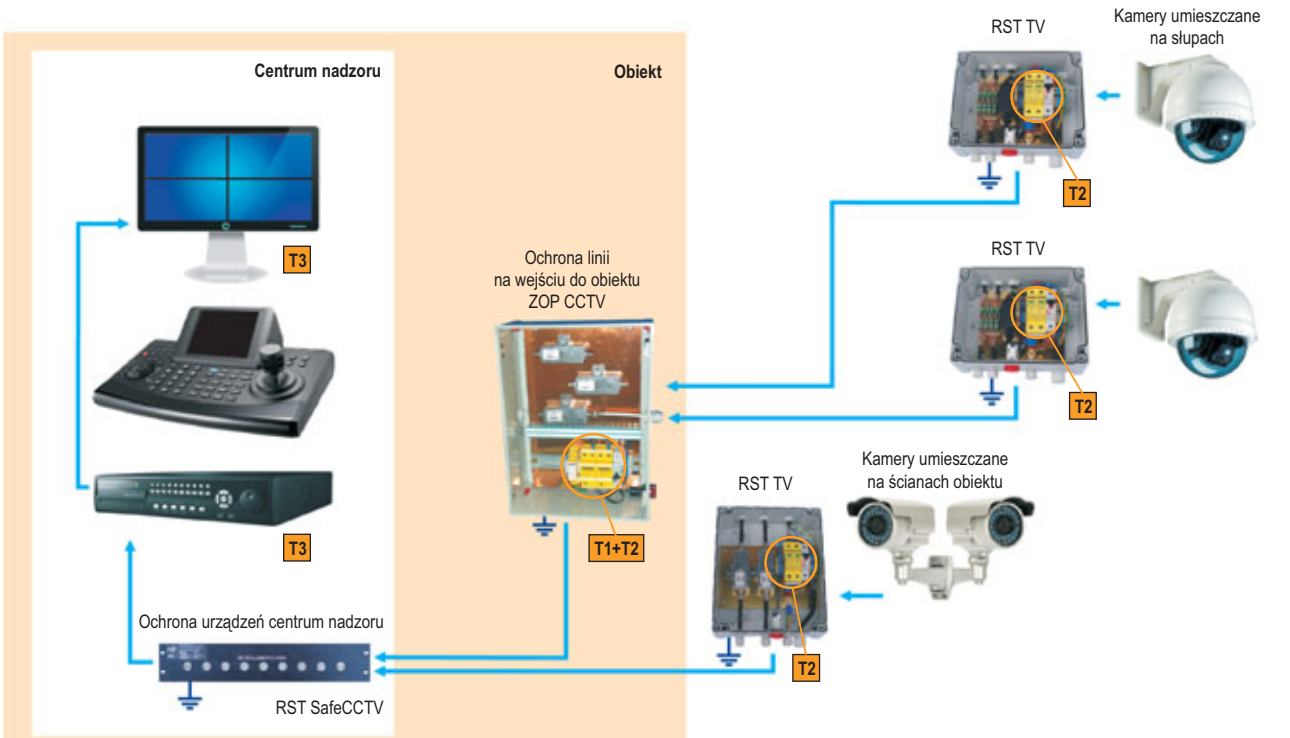
RST sp.j. z Białegostoku – dystrybutor urządzeń oraz dostawca kompleksowych rozwiązań służących do ochrony przed przepięciami i ochrony odgromowej oferuje gotowe urządzenia do zabezpieczania systemów dozorowych CCTV. Układy RST TV, ZOP CCTV i RSTsafeCCTV umożliwiają skuteczną ochronę i zwiększają niezawodność systemów nadzoru wizyjnego pracujących w środowisku, w którym są narażone na przepięcia lub oddziaływanie częściowych prądów piorunowych. Oferowane układy zapewniają ochronę zarówno linii zasilających, jak i sygnałowych. Układy te mieszczą się we wspólnej obudowie. Spośród wszystkich dostępnych na polskim rynku urządzeń tego typu wyróżniają się najwyższą skutecznością ochrony. Takie rozwiązanie znacząco ułatwia realizację strefowej koncepcji ochrony przed przepięciami zgodnie z obowiązującymi normami PN-EN 62305 dotyczącymi ochrony odgromowej. Stosowanie gotowych układów ochronnych ułatwia projektowanie, pozwala uniknąć błędów podczas montażu i gwarantuje pewność działania ograniczników przepięć. Produkty są wyposażone w podzespoły renomowanych firm, takich jak niemiecka firma LEUTRON oraz amerykańska PolyPhaser (Transtector). Ogólna koncepcja ochrony systemu dozorowego CCTV z wykorzystaniem gotowych układów ochronnych produkcji RST jest przedstawiona na rysunku 1.

RST TV

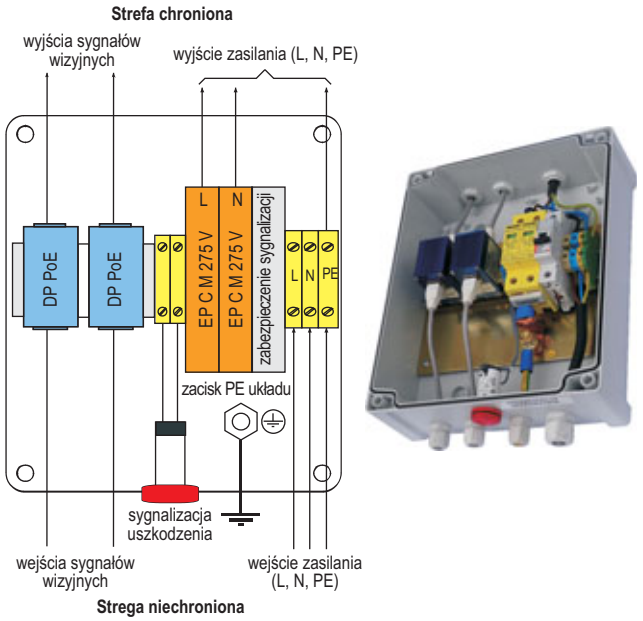
Umieszczone w jednej obudowie układy RST TV zapewniają kompletną ochronę kamer zarówno od strony linii zasilającej, toru wizyjnego, jak i sterowania. Układy te są przeznaczone do bezpośredniego zabezpieczenia kamer znajdujących się na słupach lub kamer umieszczanych na zewnętrznych ścianach budynków (w tym przypadku stanowią jednocześnie ochronę przed przepięciami na granicy stref LPZ 0/1). Układy są przystosowane do ochrony przeciwprzepięciowej klasycznych linii zasilających i sygnałowych w kamerach CCTV, ale można je dostosować także do dowolnej innej konfiguracji sprzętowej. W tabeli 1 przedstawiono typowe symbole używane przy oznaczaniu produktów oferowanych przez naszą firmę. Podam przykład. RST TV C/230$_{AC}$/8S/UV to układ przeznaczony do ochrony kamer zasilanych napięciem przemiennym 230 V. Sygnał wizyjny jest przesyłany kablem koncentrycznym z interfejsem RS485. Całość jest umieszczona w odpornej na promieniowanie UV obudowie o stopniu szczelności IP66. Standardowo układy RST TV są przeznaczone do ochrony pojedynczych kamer, ale można stworzyć i zamknąć w jednej obudowie układ zabezpieczający większą liczbę kamer, np. jeżeli są one umieszczone na jednym słupie lub bardzo blisko siebie (np. na narożniku budynku). Takie rozwiązanie umożliwia znaczne zmniejszenie kosztów ochrony całego systemu. Przykładowy układ RST TV/2xIP/230$_{AC}$/0/UV służący

RST TV / [1] / [2] / [3] / [4]	
Symbol	**Oznaczenie**
[1] sposób transmisji sygnału wizyjnego	
C	przewód koncentryczny 75 Ω
P	para żył
IP	Ethernet + PoE
[2] napięcie zasilające kamerę	
230AC	napięcie przemienne 230 V
24DC	napięcie stałe 24 V
[3] sposób sterowania ruchem kamery	
8S	interfejs RS485, 2-żyłowy
2D	interfejs RS422, 2-żyłowy
0	kamera stacjonarna
[4] rodzaj obudowy układu	
UV	odporna na promieniowanie UV, IP 66
S	standardowa, IP 65

Tab. 1. Oznaczenie układów RST TV



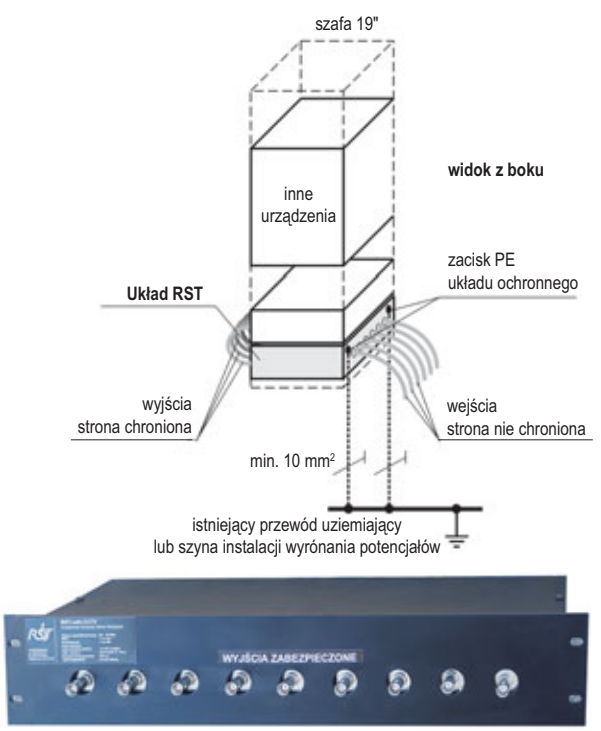
Rys. 1. Koncepcja ochrony przed przepięciami systemu CCTV



Rys. 2. Układ ochronny RST TV/2xIP/230AC/0/UV

do ochrony dwóch kamer sieciowych z interfejsami Ethernet przedstawiono na rysunku 2.

Ochrona zasilania jest oparta na zastosowaniu ograniczników przepięć typu 2 (klasy C, [T2]) firmy LEUTRON. Standardowe układy są przeznaczone do zabezpieczania kamer zasilanych napięciem przemiennym 230 V lub napięciem stałym 24 V. W każdym układzie znajduje się zewnętrzny wskaźnik sprawności ochrony linii zasilającej wykorzystujący styki sygnalizacyjne ograniczników przepięć. Umieszczona w widocznym miejscu, na zewnątrz obudowy, lampka sygnalizuje uszkodzenie elementu ograniczającego przepięcia. Dzięki takiemu rozwiązaniu można w prosty i szybki sposób skontrolować stan układu ochronnego, nawet jeżeli jest on umieszczony w trudno dostępnym miejscu.



Rys. 3. Układ ochronny RST SafeCCTV (panel ochronny oraz sposób montażu)

Elementy służące do ochrony torów wizyjnych i obwodów sterowania dobierane są w zależności od standardów, którym odpowiada dana kamera. Do transmisji sygnałów wizyjnych wykorzystuje się kabel koncentryczny, lub okablowanie strukturalne. Ponadto w pewnych przypadkach konieczna jest transmisja sygnałów sterujących ruchem kamer obrotowych. Układy RST TV mogą być dostosowane do dowolnego sposobu sterowania kamerami z wykorzystaniem zarówno interfejsów RS485, jak i RS422.

Standardowo wszystkie elementy służące do ograniczania przepięć zapewniają ochronę przed indukowanymi prądami wyładowczymi (i_{SN}) o kształcie 8/20 μs i wartościach szczytowych około 20 kA. Przykładowe parametry układu przedstawiono w tabeli 2. W zależności od wymagań wobec projektowanego układu możliwe jest wykonanie zabezpieczeń z zastosowaniem ograniczników przepięć o podwyższonej odporności udarowej, np. z ogranicznikami przepięć typu 1+2 ([T1+T2]) w torze zasilania, które są zdolne do częściowego odprowadzenia prądów pioruna (10/350 μs). Konieczność zabezpieczenia przed tak dużymi prądami może pojawić się w przypadku umieszczenia

RST TV/C/230AC/8S/UV		
Wymiary (wys. x szer. x gł.)	mm	270 x 185 x 175
Stopień ochronności obudowy		IP66
Odporność na promieniowanie UV		tak
Zacisk do podłączenia PE		śruba M10
TOR WIZYJNY		
Liczba chronionych żył		1
Napięcie znamionowe	U_N	1,5 V_{p-p}
Impedancja falowa	Z	75 Ω
Prąd maksymalny DC	I_{MAX}	2 A
Znamionowy prąd wyładowczy (8/20)	i_{sn}	18 kA
Energia odprowadzana przy i_{sn}	E_o	110 J
Energia przenikająca przez element	Ep	≤ 103 μJ
Pasmo przepustowe	f_G	DC -30 MHz
VSWR w paśmie przepustowym (maks.)		1.1
Tłumienie w paśmie przepustowym		≤ 0,3 dB
Sposób uziemienia ekranu		przez iskiernik
ZASILANIE		
Liczba gałęzi ochrony		1
Napięcie znamionowe	U_N	230/400 V_{AC}
Największe trwałe napięcie pracy	U_C	275 V AC, 350 V_{DC}
Napięciowy poziom ochrony przy udarze 5 kA (8/20 μs)	U_p	≤ 1000 V
Czas zadziałania	t	≤ 25 ns
Znamionowy prąd wyładowczy 8/20 μs	i_{sn}	20 kA
Maksymalny prąd wyładowczy 8/20 μs	i_{max}	40 kA
Maksymalny prąd zabezpieczeń obwodu chronionego	I_N	125 A gL/gG
STEROWANIE		
Liczba chronionych żył		2
Napięcie znamionowe	U_N	12 V
Największe trwałe napięcie pracy	U_C	14,5 V_{DC}, 10,2 V_{AC}
Prąd znamionowy	I_N	1 A
Znamionowy prąd wyładowczy (8/20)	i_{sn}	20 kA
Napięciowy poziom ochrony przy 1 kV/μs / i_{sn}	U_p	≤ 19 V/≤ 600 V
Temperatura pracy	T	-25 °C ... +85 °C

Tab. 2. Przykładowe parametry układu

Liczba chronionych linii			1 … 9
Napięcie znamionowe		U_N	1,5 V_{p-p}
Impedancja falowa		Z	75 Ω
Prąd maksymalny DC		I_{MAX}	2 A
Znamionowy prąd wyładowczy (8/20)		i_{sn}	18 kA
Energia odprowadzana przy i_{sn}		E_o	110 J
Energia przenikająca przez element		E_p	≤ 103 μJ
Pasmo przepustowe		f_G	DC - 30 MHz
Tłumienie w paśmie przepustowym			≤ 0,3 dB
VSWR w paśmie przepustowym (maks.)			1.1
Złącze typu	wej/wyj		BNC
Temperatura pracy			-45 ÷ +45 °C
Wymiary (wys. x szer. x gł.)		mm	(2Ux19")
Zacisk do podłączenia PE			Śruba mosiężna M8

Tab. 3. Parametry układu RSTsafe

kamer na wieżach telekomunikacyjnych lub stacjach energetycznych średnich i wysokich napięć, które coraz częściej obejmowane są stałym nadzorem wizyjnym.

ZOP CCTV

Do ochrony linii odchodzących od słupów kamerowych wprowadzanych do budynku (na granicy stref LPZ 0/1) doskonale nadają się złącza ochrony przed przepięciami ZOP CCTV. Układy te umożliwiają wprowadzenie i zabezpieczenie wszystkich linii wchodzących do obiektu w jednym punkcie i pewne uziemienie tego punktu, które jest gwarancją prawidłowego działania zastosowanych ograniczników przepięć. Układy te mają podobną budowę i parametry jak RST TV i mogą być dostosowane do dowolnej liczby kamer. Standardowo do ochrony obwodów zasilania w układach ZOP CCTV stosuje się ograniczniki przepięć typu 1 + 2 ([T1+T2]).

RST SafeCCTV

RST SafeCCTV to jedyny dostępny na rynku kompaktowy ogranicznik przepięć o odporności aż 18 kA, przeznaczony do ochrony koncentrycznych torów wizyjnych urządzeń zainstalowanych w centrum nadzoru wizyjnego. Układ ten jest przedstawiony na rysunku 3. Zastosowano w nim ograniczniki przepięć firmy PolyPhaser. Układ jest umieszczony w metalowej obudowie przystosowanej do montażu w szafach aparaturowych w standardzie 19". Pojedynczy układ pozwala na zabezpieczenie do dziewięciu torów wizyjnych. Takie rozwiązanie umożliwia skuteczne zabezpieczenie takich urządzeń jak rejestratory lub multipleksery, do których doprowadzane są wszystkie tory wizyjne kamer CCTV.

Opracowanie: dr inż. Tomasz Maksimowicz

RST sp.j.
ul. Myśliwska 2, 15-569 Białystok
tel.: 85 741 08 80, faks: 85 741 09 69
e-mail: rst@rst.pl
www.rst.pl

Oferta Axisa skierowana do instalatorów niewielkich systemów nadzoru wizyjnego

Axis Communications

AXIS Camera Companion jest bezpłatnym systemem do zarządzania materiałem wizyjnym, znajdującym zastosowanie w małych instalacjach zawierających od kilku do kilkunastu kamer. Cechuje go prostota konstrukcji, liczba elementów składowych została ograniczona do niezbędnego minimum, a oprogramowanie sieciowe jest łatwe do skonfigurowania

Fot. 1. Możliwość skontrolowania obiektu za pośrednictwem urządzeń przenośnych jest dostępna wszędzie i zawsze co stwarza swoiste poczucie bezpieczeństwa

AXIS Camera Companion jest nowym rozwiązaniem, dzięki któremu użytkownicy końcowi mogą czerpać wszelkie korzyści wynikające z zalet telewizji cyfrowej. Do tych zalet należą: wysoka jakość obrazu, zbliżona do jakości oferowanej przez domowe odbiorniki telewizyjne pracujące w standardzie HDTV, wyświetlanie obrazów w czasie rzeczywistym, łatwy w użyciu interfejs graficzny służący do obsługi systemu, możliwość oglądania obrazów na urządzeniach przenośnych i telefonach komórkowych. To wszystko na pewno przyciągnie wielu klientów, a tym samym może przyczynić się do zwiększenia popytu na proste telewizyjne systemy dozorowe.

System AXIS Camera Companion ma pewne funkcje, które są niedostępne w klasycznych systemach antywłamaniowych opierających swoje działanie na czujkach ruchu. Do tych funkcji należą: identyfikacja intruzów wykrytych na chronionym obszarze, automatyczne powiadamianie służb ochrony lub użytkowników końcowych o konieczności podjęcia interwencji i załączenie odpowiedniego materiału zdjęciowego.

Oferta Axisa uwzględnia potrzeby użytkowników końcowych

Właściciele małych firm z natury rzeczy nie są rozrzutni, jednak są zainteresowani wizyjnymi systemami dozorowymi oferującymi obraz o wysokiej jakości, typowej dla współczesnych domowych odbiorników HDTV. Równie istotny jest dla nich komfort wynikający z możliwości zdalnego monitorowania chronionych obiektów z użyciem urządzeń mobilnych i telefonów komórkowych. Stwarza to poczucie bezpieczeństwa. Epoka telefonów z obrotową tarczą, a nawet telefonów z klawiaturą numeryczną, minęła. Współczesne smartfony oferują wiele nowych funkcji, które mogą być przydatne w systemach monitoringu wizyjnego.

System dozorowy AXIS Camera Companion ma prostą budowę i jest łatwy w obsłudze

W systemach AXIS Camera Companion nie zostały wyodrębnione żadne jednostki centralne, zaś wszystkie funkcje użytkowe są realizowane przez kamery. Dotyczy to zarówno możliwości wykrywania i identyfikacji intruzów w chronionych obiektach, jak i możliwości pobierania strumieni danych bezpośrednio z kamer. W praktyce oznacza to, że w systemach dozorowych AXIS Camera Companion nie są stosowane żadne rejestratory wizyjne ani jednostki centralne zarządzające ich pracą. Wysoka jakość uzyskiwanych obrazów pozwala na realną ocenę sytuacji w chronionych obiektach, zaś automatyzacja funkcji alarmowych umożliwia realizację zadań typowych dla klasycznych systemów alarmowych.

Koncepcja działania systemu AXIS Camera Companion

W skład systemu AXIS Camera Companion wchodzą kamery Axis z zainstalowanymi kartami pamięci SD. Niezbędne są także elementy tworzące lokalną sieć IP, takie jak przełączniki sieciowe, rutery z bramkami internetowymi oraz oprogramowanie klienckie komputerów PC i urządzeń mobilnych. Materiał wizyjny jest zapisywany bezpośrednio

Fot. 2. Krystalicznie czysty obraz HDTV zawiera szczegóły pozwalające na identyfikację obserwowanych osób – takich możliwości nie miały systemy analogowe

na kartach SD znajdujących się w kamerach, dzięki czemu każdą z tych kamer można traktować jak niezależne urządzenie dozorowe. Oznacza to, że nie zachodzi konieczność stosowania jakichkolwiek rejestratorów typu DVR, NVR czy komputerów rejestrujących obrazy na dyskach twardych. Dzięki temu system AXIS Camera Companion ma prostą konstrukcję, jest tani i łatwy w instalacji. Wykorzystywane w nim oprogramowanie klienckie automatycznie wykrywa wszystkie dostępne kamery i umożliwia ich szybką konfigurację. Stosując smartfony, tablety, laptopy lub komputery PC, zyskuje się możliwość obserwacji obrazów w czasie rzeczywistym i dosłownie w każdym miejscu, w którym uzyska się dostęp do Internetu.

Działanie systemu AXIS Camera Companion jest proste i niezawodne. Wszystkie kamery są zasilane metodą PoE, dzięki czemu wystarczy zapewnić niezawodne zasilanie przełącznikom sieciowym i ruterowi, aby podtrzymać działanie całego systemu. Wszystkie urządzenia wraz z zasilaczem UPS mogą być umieszczone we wspólnej, ukrytej szafce instalacyjnej. Takie rozwiązanie jest szczególnie korzystne w lokalizacjach, w których zdarzają się częste

Fot. 3. Istnieje możliwość obserwacji obrazów z wielu kamer na ekranie podzielonym na 2 do 6 części w przypadku urządzeń przenośnych i na ekranie podzielonym na 4, 9 lub 16 części w przypadku komputerów PC

odłączenia od sieci energetycznej, na przykład na terenach podmiejskich.

W systemie AXIS Camera Companion może pracować większość sieciowych kamer Axis, w tym kamery o wysokiej rozdzielczości. Mogą być w nim wykorzystywane także kodery wizyjne z podłączonymi do nich kamerami analogowymi. Kodery Axis są także wyposażone we własne karty pamięci SD, dlatego mogą służyć jako lokalne rejestratory wizyjne dla kamer analogowych. Rejestracja obrazów na kartach SD umieszczonych w kamerach i koderach może być prowadzona w sposób ciągły lub wyzwalana w momencie wykrycia ruchu w obserwowanym miejscu. W skład systemu AXIS Camera Companion może wchodzić maksymalnie szesnaście kamer. Zarejestrowane obrazy mogą być odtworzone przez komputer z oprogramowaniem klienckim lub przez urządzenia mobilne, więc możliwa jest realizacja funkcji typowych dla systemów, w skład których wchodzą klasyczne rejestratory wizyjne.

Dostępność oprogramowania AXIS Camera Companion

Komputer PC z zainstalowanym oprogramowaniem klienckim AXIS Camera Companion może obsłużyć maksymalnie szesnaście kamer. Wspomniane oprogramowanie jest udostępniane na stronie WWW firmy Axis i może być użytkowane bez konieczności wykupienia licencji.

By ułatwić projektowanie systemów dozorowych i umożliwić dostosowanie ich funkcji do potrzeb użytkowników końcowych, firma Axis opracowała oprogramowanie narzędziowe AXIS Camera Companion Buyers Tool, które także jest nieodpłatnie dostępne dla wszystkich nabywców kamer Axis. To oprogramowanie pozwala na łatwy dobór liczby i rodzaju kamer Axis niezbędnych do budowy systemów dozorowych spełniających wymagania stawiane przez użytkowników końcowych. Umożliwia także dobór sprzętu sieciowego i innych składników niezbędnych do zbudowania instalacji zawierających określoną liczbę kamer.

Osoby zainteresowane praktycznym wykorzystaniem oprogramowania AXIS Camera Companion Buyers Tool mogą wejść w posiadanie wszystkich jego składników, zanim zakupią kamery i sprzęt sieciowy. Oprogramowanie można uruchomić na próbę na dowolnym komputerze, co pozwala na szybkie zapoznanie się z funkcjonowaniem systemu dozorowego AXIS Camera Companion bez konieczności ponoszenia jakichkolwiek kosztów. Na podobnej zasadzie instalatorzy mogą prezentować system AXIS Camera Companion użytkownikom końcowym, co stwarza klarowną sytuację na etapie składania oferty.

System dozorowy AXIS Camera Companion został zaprojektowany z myślą o masowym odbiorcy, zaś jego upowszechnienie przyczyni się do podwyższenia poziomu bezpieczeństwa małych i średnich obiektów, zarówno mieszkalnych, jak i użytkowych. Prostota obsługi oraz automatyzacja czynności związanych z identyfikacją potencjalnych intruzów umożliwia korzystanie z systemu AXIS Camera Companion przez osoby nieprzeszkolone. Szczegółowy opis systemu można znaleźć na stronie WWW firmy Axis.

Axis Communications

Większa rentowność dzięki dyskretnemu i przystępnemu cenowo rozwiązaniu do nadzoru z funkcjami PTZ? **To proste.**

Czy chcą Państwo poprawić bezpieczeństwo w swoim sklepie? A może także zwiększyć efektywność operacyjną i rentowność? Oba te cele pomoże zrealizować rozwiązanie nadzoru wizyjnego.

Kamery Axis z linii M z funkcjami obrót/pochylenie/zbliżenie udostępniają materiał wizyjny jakości HDTV, alarmy w czasie rzeczywistym oraz inne inteligentne i przydatne możliwości. Dzięki nim można między innymi zwalczać kradzieże w sklepach, zapobiegać brakowi towaru na półkach oraz monitorować kolejki do kas.

Ze względu na elastyczne funkcje obrót/pochylenie/zbliżenie, niewielkie rozmiary i prostą instalację kamery AXIS z serii M50 umożliwiają łatwą i dyskretną obserwację wszystkiego, co dzieje się w sklepie.

Niewielka kamera. Wielkie możliwości. Łatwy wybór.

Przyjmij punkt widzenia Axis. Bądź zawsze o krok do przodu.
Odwiedź www.axis.com/ptz

Kopułkowa kamera sieciowa PTZ AXIS z serii M50 • Jakość materiału wizyjnego do poziomu HDTV 720p • Funkcje obrotu, pochylenia i zbliżenia oraz ultradyskretna konstrukcja • Zasilanie przez sieć Ethernet • Wbudowany mikrofon • Ochrona klasy IP51 • Gniazdo kart pamięci MicroSD/SDHC

AXIS COMMUNICATIONS

System kontroli dostępu
Kaba exos 9300
z funkcją CardLink

Rafał Tamborski

Fot. 1. Terminal rejestracji czasu pracy B-web 9300

Na tegorocznych targach SECUREX firma Kaba otrzymała złoty medal za system kontroli dostępu Kaba exos 9300 z funkcją CardLink. CardLink jest z jednym z modułów systemu kontroli dostępu Kaba exos. To innowacyjne rozwiązanie nie wymaga okablowania. Polega na przeniesieniu danych autoryzacyjnych bezpośrednio na nośnik – kartę zbliżeniową lub klucz inteligentny. Dzięki temu można powiązać działające on-line punkty dostępowe systemu ACC z autonomicznymi zamkami zasilanymi bateryjnie. CardLink umożliwia zatem jednoczesne i takie same zarządzanie autonomicznymi zamkami systemowymi oraz punktami dostępowymi systemu kontroli dostępu pracującymi on-line. Wszystko to w jednym systemie

Firma Kaba Polska funkcjonuje od 2001 r. i jest jedną z firm szwajcarskiej spółki giełdowej Kaba Holding specjalizującej się w produkcji mechanicznych, mechatronicznych i elektronicznych systemów zamknięć i kontroli dostępu. Prawie 60 spółek Kaba na całym świecie, które wyspecjalizowały się w różnych dziedzinach kontroli dostępu, zapewnia klientom dostęp do nowoczesnych technologii znajdujących zastosowanie wszędzie tam, gdzie obowiązują najwyższe wymagania dotyczące bezpieczeństwa i jakości. Grupa Kaba obchodzi w tym roku 150-lecie istnienia na rynku.

Główne grupy produktów firmy Kaba to:

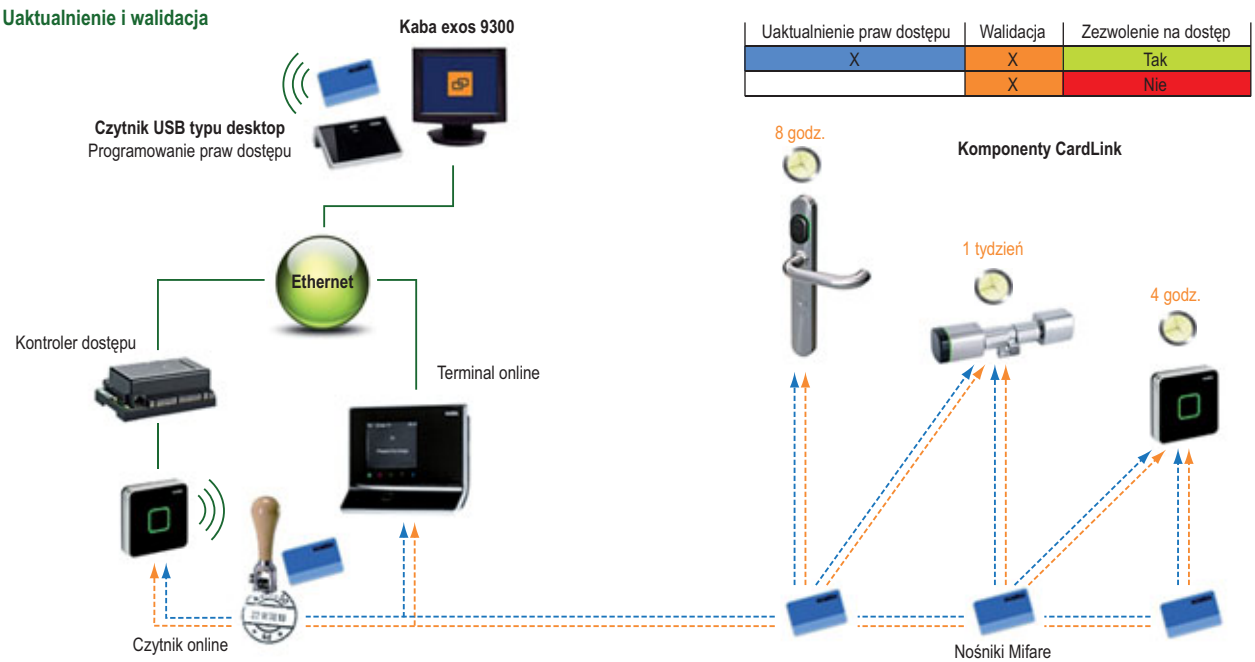
– elektroniczne systemy kontroli dostępu i rejestracji czasu pracy,
– urządzenia do fizycznej kontroli dostępu (tripody, bramki uchylne, bramki obrotowe, bramki szybkiego przejścia, drzwi karuzelowe, śluzy, furty stadionowe),
– zamki mechaniczne i mechatroniczne,
– systemy master key,
– elektroniczne zamki hotelowe,
– depozytory kluczy.

Kaba exos 9300

System kontroli dostępu Kaba exos 9300 to zintegrowane, kompleksowe rozwiązanie do automatycznej kontroli dostępu i wejść, zarządzania alarmami, rejestracji czasu pracy i gromadzenia danych przedsiębiorstwa. System standardowy można wykorzystać do rozszerzenia na całą firmę. Obejmuje całą niezbędną kontrolę dostępu oraz funkcje alarmu i rejestrowania. Można dostosowywać go do zmieniających się wymogów organizacyjnych i dotyczących bezpieczeństwa. Modułowa budowa systemu umożliwia idealne dostosowanie go do wymagań klienta.

Moduły:

– system standardowy,
– personalizacja kart zbliżeniowych,
– zarządzanie przejściami,
– zarządzanie depozytorami kluczy,
– kontrola dostępu,
– zarządzanie parkingiem,
– serwer OPC,
– CardLink,
– interfejs do mySAP,
– zarządzanie gośćmi,
– B-Comm ERP dla SAP,
– rejestracja czasu pracy,
– zarządzanie klientami,
– klient sieci WWW,
– zarządzanie kartami zbliżeniowymi,
– uaktualnienie licencji.



Karty zbliżeniowe, które nie są przypisane do żadnej osoby mogą być dewalidowane przy pomocy czytnika desktop. Dewalidacja kasuje prawa dostępu. Wtedy karta zbliżeniowa nie ma zezwolenia dostępu do komponentów Cardlink.

Rys.1. Graficzne przedstawienie sposobu działania systemu CardLink

Fot. 2. Czytniki – RFID SL z PIN i bez

CardLink

Jednym z modułów, który można wykorzystać w systemie kontroli dostępu, jest CardLink. Moduł ten powiązuje system kontroli dostępu działający on-line z autonomicznymi komponentami mechatronicznymi i umożliwia skonfigurowanie elementów pracujących on-line i komponentów autonomicznych centralnie, w jednym miejscu. Do zarządzania wszystkimi komponentami i ich konfigurowania służy wspólna aplikacja. Dane wpisywane są tylko raz. Poszczególni użytkownicy systemu uzyskują uprawniony dostęp do wybranych komponentów. Administrator ma w każdej chwili dostęp do informacji o wszystkich przydzielonych uprawnieniach. Może je w jednolity sposób i w każdej chwili dokumentować.

Innowacyjne mechanizmy CardLink przechowują informacje o prawach dostępu poszczególnych użytkowników systemu do poszczególnych komponentów autonomicznych bezpośrednio na nośniku. Zezwolenia są odczytywane i oceniane przez autonomiczne komponenty CardLink na miejscu w celu ustalenia, czy dostęp jest dozwolony. Mechanizm ten jest wykorzystywany także w celu sprawdzenia, czy te uprawnienia są ważne. Jeżeli niezbędna będzie aktualizacja praw dostępu, użytkownik zostanie o tym poinformowany. Aktualizacji dokonuje się za pośrednictwem czytnika pracującego on-line lub komputera PC. Nie ma potrzeby przeprogramowywania komponentów autonomicznych, gdy ktoś zgubi kartę lub trzeba wydać kartę dla gościa.

Powiązanie elementów pracujących on-line i autonomicznych umożliwia zmniejszenie kosztów inwestycji. W miejscach, do których dostęp ma określona, ciągle ta sama grupa ludzi (a więc nie trzeba często dokonywać korekty uprawnień), można użyć komponentów autonomicznych. Dotyczy to np. drzwi wewnątrz budynku. Włączone do systemu kontroli dostępu on-line drzwi zewnętrzne do budynku zwiększają poziom bezpieczeństwa obiektu i zostaną powiązane z komponentami autonomicznymi. CardLink gwarantuje maksymalną efektywność działania w codziennym użytkowaniu, dając praktycznie nieograniczone możliwości rozbudowy.

Tylko uwierzytelnione karty zbliżeniowe mogą aktywować działanie komponentów autonomicznych. Okres ważności może być ustalony w zależności od wymagań związanych z bezpieczeństwem. Po upływie tego okresu dane na karcie tracą ważność. Jeśli karta zostanie zgubiona, nieautoryzowany dostęp zostanie uniemożliwiony poprzez jej dezaktywację. Można również stworzyć kartę blokującą – do natychmiastowego zablokowania dostępu. CardLink rejestruje wszystkie zdarzenia w taki sposób, by nie można było zmienić dotyczących ich informacji.

Rafał Tamborski
Kaba

OCHRONA OBWODOWA OBIEKTÓW CCTV

ZBAR

_ CCTV

- kamery laserowe
- kamery termowizyjne
- hybrydowe kamery termowizyjne w technologii laserowej
- systemy transmisji światłowodowej
- rejestratory: DVR, NVR, hybrydowe (DVR/NVR), mobilne DVR
- kamery IP i analogowe
- systemy ścian wideo „video wall"

„Xpanse Video Wall"– najnowszy system ścian wideo

- obsługuje kamery analogowe oraz IP
- prosta konfiguracja wyglądu ściany wideo
- zestaw gotowy do uruchomienia
- max 40 monitorów (plazmowych, LCD lub projektorów)
- przekątne monitorów od 38 do 110 cali
- kontroler z oprogramowaniem „Xpanse control"
- oprogramowanie „Xpanse client" dla operatorów
- sześciordzeniowy procesor Intel Xeon
- 24GB pamięci operacyjnej
- konfigurowalny układ monitorów
- złącza: USB, VGA, HDMI, DVI, BNC, S-Video, Ethernet

94-214 Łódź, Poland, Krakowska 60
Tel. + 48 **426 111 298**, Fax +48 **426 111 297**
e-mail: zbar@zbar.com.pl

sprawdź pełną ofertę na **www.zbar.com.pl**

Aventura · FFT · Protech · CIAS · SCHRACK SECONET · SENSTAR · GPS · IFTER

Bariery podczerwieni i czujka 3 x PIR

ATSUMI®

seria NR-TS/NR-TM

seria NR-QS/NR-QM

SIR10S

Wyłączny dystrybutor produktów Atsumi w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Red Barrier

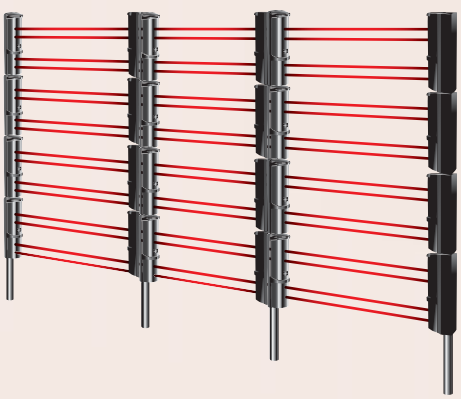
Zbuduj niewidzialny system detekcji z ATSUMI

Zewnętrzne bariery podczerwieni

dwuwiązkowe serii **NR-TS** i **NR-TM**
czterowiązkowe serii **NR-QS** i **NR-QM**

Bariery podczerwieni ATSUMI posiadają niezawodne, kontrolowane cyfrowo układy, które zapewniają bezawaryjną pracę i doskonałą ochronę nawet w najtrudniejszych warunkach środowiskowych.

- Sferyczne soczewki Fresnela
- Skuteczna detekcja nawet przy 99% poziomie tłumienia wiązki, podczas pracy w trudnych warunkach atmosferycznych (deszcz, mgła, śnieg itp.)
- Układ automatycznej regulacji wzmocnienia (AGC)
- Podwójna modulacja częstotliwości wiązki i funkcja kontroli mocy sygnału wiązki (NR-QS, NR-QM)
- Obwód EDC (NR-QS, NR-QM)
- Wybór kanału częstotliwości pracy (NR-QM, NR-TM)
- Tryb OR (NR-QM)
- Klasy szczelności IP54 (NR-QS, NR-QM) i IP55 (NR-TS, NR-TM)
- Łatwa instalacja
- Wysoce niezawodna ochrona obwodowa oparta na innowacyjnej technologii - możliwość instalacji do 4 barier w pionie (NR-QM)



Zewnętrzna pasywna czujka podczerwieni 3 x PIR

SIR10S

Czujka podczerwieni ATSUMI wykorzystuje nowo opracowaną metodę potrójnej detekcji PIR, dzięki czemu zapewnia niezawodną ochronę na zewnątrz obiektów i jednocześnie jest odporna na źródła fałszywych alarmów.

- Sferyczne soczewki Fresnela
- Zbieranie informacji przez 3 niezależne czujniki PIR
- Filtry światła białego
- Możliwość podłączenia do systemów CCTV lub innych aplikacji
- Klasa szczelności IP55
- Wszechstronność instalacji, możliwość montowania czujek jedna koło drugiej lub naprzeciwko siebie

Metoda zapobiegania fałszywym alarmom dzięki potrójnej detekcji PIR

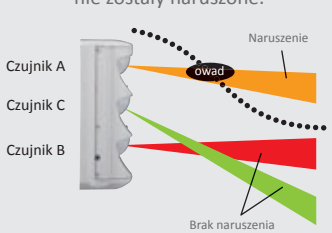
Bezpośrednie działanie promieni słonecznych

Naruszenie pól detekcji czujników A i B.
Pole detekcji czujnika C
nie zostało naruszone.

Nawet w przypadku, gdy czujniki A i B skierowane są bezpośrednio na działanie promieni słonecznych, czujka nie wchodzi w stan alarmu.

Owady, ptaki i zwierzęta

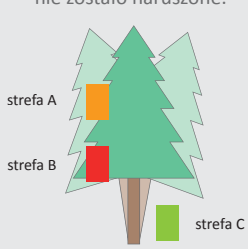
Naruszenie pola detekcji czujnika A.
Pola detekcji czujników B i C
nie zostały naruszone.



Latające ptaki, owady lub spadające z drzew liście nie powodują wejścia czujki w stan alarmu.

Poruszająca się roślinność

Naruszenie pól detekcji czujników A i B.
Pole detekcji czujnika C
nie zostało naruszone.



Kołysząca się roślinność nie powoduje wejścia czujki w stan alarmu.

Efekt synergii

Jak połączyć ze sobą ewidencję czasu pracy, kontrolę dostępu i planowanie zatrudnienia personelu

Markus Bundschuh

Globalizacja stawia przedsiębiorstwa w obliczu coraz większej konkurencji. Odpowiedzią na nią są działania mające na celu ograniczanie kosztów, a co za tym idzie zwiększenie efektywności działania przedsiębiorstwa. Systemy kontroli dostępu, rejestracji czasu pracy i planowania zatrudnienia są ważnym elementem tej strategii. Firma Interflex Datensysteme, oferująca kompleksowe systemy informatyczne, udostępnia efektywne zintegrowane rozwiązania, dzięki którym można lepiej zarządzać czasem pracy

Fot. 1. NetworkOnCard to technologia łącząca kontrolę dostępu z rejestracją czasu pracy

Wiele przedsiębiorstw dąży do racjonalizacji procesów w celu uzyskania przewagi konkurencyjnej. Pierwszym krokiem w tym kierunku może być uelastycznienie czasu pracy. Redukcja kosztów jest możliwa szczególnie w zakresie planowania zatrudnienia personelu, rejestracji czasu pracy i kontroli dostępu, zarówno dzięki podjęciu działań organizacyjnych, jak i wprowadzeniu innowacji technologicznych. Specjaliści w tej dziedzinie wiedzą, że inwestycje szybko się zwrócą, gdy umiejętnie połączy się ze sobą planowanie zatrudnienia personelu, gospodarowanie czasem i zapewnianie bezpieczeństwa. Takie połączenie jest możliwe wtedy, gdy karty elektroniczne są używane nie tylko do identyfikacji pracowników, lecz także do rejestrowania ich czasu pracy. Podstawą takiego systemu jest wprowadzenie kart jako identyfikatorów oraz zastosowanie odpowiednich terminali i czytników kart. Pracownicy nie muszą wówczas nosić przy sobie kluczy ani zapamiętywać haseł czy numerów PIN. Zastosowanie karty elektronicznej jako identyfikatora eliminuje koszty związane z koniecznością wymiany zamków w przypadku zgubienia lub kradzieży kluczy. Zdecydowaną przewagę nad konkurencją zapewnia administrowanie danymi związanymi z kontrolą dostępu i rejestracją czasu pracy w oparciu o jedno oprogramowanie. Takie rozwiązanie umożliwia także zarządzanie dodatkowymi danymi, na przykład dotyczącymi dni urlopu. Wprowadzone dane mogą być przedmiotem analiz i podstawą do sporządzania raportów. W przypadku przekroczenia ustalonych limitów, np. limitu dostępnych dni urlopu, generowane są komunikaty ostrzegawcze. System umożliwia nawet rejestrowanie czasu realizacji projektów, które mogą być przejrzyście pogrupowane w raporcie za pomocą oprogramowania planistycznego. Wyniki rejestracji czasu pracy są przekazywane za pośrednictwem zintegrowanych interfejsów do oprogramowania księgowego lub kadrowo-płacowego, np. SAP czy DATEV, w którym następuje ich dalsze przetwarzanie.

Wygodne w użyciu karty elektroniczne

Karty zbliżeniowe lub chipowe przyczyniają się do ułatwienia pracy w przedsiębiorstwie. Zintegrowana karta może mieć wiele zastosowań, np. służyć do realizacji bezgotówkowych płatności w stołówce i automatach czy sterowania windą. Ponadto za pomocą karty pracownik może zablokować swój komputer osobisty, do którego podłączony jest czytnik, gdy na krótki czas opuszcza miejsce pracy. Wybór typu karty elektronicznej należy do klienta – czytniki Interflex rozpoznają wszystkie powszechnie stosowane technologie chipowe, takie jak Mifare, LEGIC, Hitag czy Proxif.

Więcej pomysłów na większą efektywność dzięki planowaniu pracy personelu

Dane czasowe, zarejestrowane za pomocą kart, są analizowane w oparciu o specjalistyczne oprogramowanie do zarządzania kadrami. Na podstawie tych oraz innych istotnych danych sporządzane są prognozy dotyczące zapotrzebowania personalnego. Warunkiem tych kalkulacji jest dysponowanie informacjami dotyczącymi założeń budżetu, poszczególnych modeli czasu pracy, właściwych kont czasu pracy, nieobecności, planowania urlopów, zleceń oraz uwarunkowań prawnych. Możliwy jest także import danych uzupełniających, takich jak dane finansowe lub plany zasobów ogólnych przedsiębiorstwa. Planiści z łatwością opanowują obsługę oprogramowania i mają szybki wgląd we wszystkie parametry prognoz. Tym samym otrzymują narzędzie, za pomocą którego mogą łatwo i szybko opracowywać plany zmianowe oraz kadrowe na podstawie sparametryzowanych tablic i okien planistycznych. Rozwiązanie to umożliwia na przykład łatwiejszą identyfikację obniżonych mocy przerobowych, co z kolei pozwala wyeliminować kosztowne nadgodziny. Ujęcie w planach indywidualnych potrzeb pracowników ułatwia im połączenie życia zawodowego i prywatnego. Oprogramowanie wspomaga ponadto poszczególne działy przy obliczaniu krótko-, średnio- i długoterminowego zapotrzebowania personalnego. Ma to tę zaletę, że można szybko reagować na krótko- i długotrwałe trendy oraz elastycznie dopasowywać do nich procesy. Dzięki szybszemu planowaniu koszty operacyjne każdej jednostki przedsiębiorstwa zostaną obniżone.

Budowa i centralne administrowanie wewnętrznymi rezerwami

W razie zwolnień chorobowych lub wahań wolumenu zleceń tworzone są tzw. grupy pracowników rezerwowych (ang. *flexpools*). Wewnętrznymi grupami pracowników rezerwowych zarządza się za pomocą specjalnie opracowanego modułu oprogramowania, dzięki któremu mogą one przystąpić do pracy tam, gdzie właśnie są potrzebne. Planiści mają zawsze do dyspozycji kilka osób rezerwowych i mogą dodatkowo zasilać rezerwy pracownikami z zewnątrz. Każdy kierownik działu lub zmiany samodzielnie decyduje, kto i kiedy ma przystąpić ma do grupy rezerwowej. Dzięki oprogramowaniu ma wgląd w profil kwalifikacji pracownika rezerwowego. Dział przedsiębiorstwa mający w danym momencie zwiększone zapotrzebowanie personalne i wymagający rezerwowych pracowników musi na czas wprowadzić informacje o tym, jakimi umiejętnościami i jaką wiedzą muszą oni dysponować. Transparentna organizacja pracy wydłuża efektywny czas pracy bez konieczności zlecania nadgodzin. To z kolei przyczynia się do poprawy zadowolenia klientów, jak również poprawia samopoczucie i motywację pracowników. Dzięki bardziej elastycznemu zarządzaniu kadrami planiści i przełożeni uzyskują też większą przejrzystość procesów organizacyjnych. Odtąd łatwiej jest mierzyć i porównywać koszty związane z wytwarzaniem produktów lub wykonywaniem usług. Zakłady zapobiegają w ten sposób problemom jakościowym i nie muszą już odmawiać realizacji zleceń z powodu braku dostatecznych mocy przerobowych. Poprzez powiązanie kontroli dostępu i ewidencji czasu pracy oraz dzięki oprogramowaniu do planowania pracy personelu przedsiębiorstwa zwiększają swą konkurencyjność i efektywność czasu pracy oraz redukują koszty.

Markus Bundschuh
Interflex Datensysteme
var-team@eu.irco.com

Partnerem Interflex w Polsce jest:
POLLDA Sp. z o.o.
ul. Wolności 311, 41-800 Zabrze
tel. 032 271 35 00, tel/fax: 032 271 64 20
www.pollda.pl

JABLOTRON 100

nowy system alarmowy firmy Jablotron Alarms

Piotr Panek

W maju 2012 roku wprowadzono do sprzedaży w Polsce nowy system firmy Jablotron Alarms. Podobnie jak w przypadku wcześniejszych produktów tej firmy, w systemie tym wykorzystano wiele innowacyjnych rozwiązań. Jest to kolejny duży krok w rozwoju Jablotron Alarms i kolejny wyraz dążenia do ugruntowania pozycji lidera na europejskim rynku

Fot. 1. Klawiatura z segmentami modułowego sterowania

Dotychczas Jablotron Alarms kojarzony był głównie z systemami bezprzewodowymi, które zdobyły uznanie instalatorów oraz wiele prestiżowych nagród na całym świecie. System JABLOTRON 100 opracowano z uwzględnieniem wyników badań rynku określających potrzeby instalatorów i użytkowników. Prace nad jego tworzeniem rozpoczęły się w 2008 roku. Jak wynikało z badań potrzeb klientów, instalatorzy oczekują urządzeń, które można szybko zamontować i które odpowiadają wymogom konkretnej instalacji, natomiast użytkownicy oczekują systemu prostego w obsłudze, szczególnie w przypadku alarmów wielostrefowych, do obsługi których konieczne było zapamiętanie kolejnych, powiązanych ze sobą czynności. Wyniki badań umożliwiły opracowanie systemu, który jest elastyczny, funkcjonalny, łatwy w instalacji, konfiguracji i obsłudze. Co to znaczy? Po pierwsze można go zastosować zarówno w małej, średniej, jak i dużej instalacji. Po drugie – można go skonfigurować na wiele sposobów. Po trzecie – jest przejrzysty dla instalatora, jego właściwości i funkcje są opisane w odpowiednich dokumentach, a użytkownik nie będzie mieć problemu z jego obsługą.

Sercem systemu JABLOTRON 100 jest centrala sterująca wyposażona w komunikator GSM i GPRS, dwa wejścia dla czterożyłowej magistrali BUS oraz oddzielne wejście umożliwiające przyłączenie modułu radiowego bezpośrednio do płyty głównej. Centrala łączy w sobie zalety kontrolera instalacji przewodowej wykorzystującej adresowalną magistralę cyfrową, która umożliwia łatwe i szybkie układanie instalacji, z zaletami kontrolera instalacji bezprzewodowej. W obydwu przypadkach kluczowe znaczenie ma skuteczny, ekspresowy i bezpieczny protokół transmisyjny, opracowany w całości przez Jablotron Alarms. Wielkość i struktura systemu są określone jedynie liczbą wykorzystanych adresów cyfrowych. System JABLOTRON 100 umożliwia podłączenie 120 adresowalnych urządzeń na pojedynczej czterożyłowej magistrali. Instalator nie musi już pamiętać o parametryzowaniu linii – kolejne urządzenia przewodowe są dołączane do magistrali. Jest to zupełnie inne podejście niż w przypadku central analogowych, gdzie każdemu pojedynczemu elementowi systemu alarmowego odpowiada oddzielne wejście lub wyjście centrali, a odpowiadający opisywanemu systemowi JABLOTRON 100 system analogowy potrzebuje aż 120 wejść i do każdego z nich musi zostać podłączona oddzielna para przewodów sygnałowych.

W miejscach, do których doprowadzenie przewodów może być trudne lub niemożliwe, można zastosować czujki bezprzewodowe. Aby zapewnić bezprzerwową, niezawodną łączność z czujkami rozmieszczonymi w całym obiekcie, do magistrali cyfrowej można włączyć do trzech modułów łączności bezprzewodowej, co pozwala na przezwyciężenie problemów związanych z zanikami propagacji fal radiowych. O jakości protokołu łączności może również świadczyć brak opóźnień i kolizji w systemie przy jego pełnym obciążeniu.

Ze względu na bardzo niewielki pobór prądu oraz oszczędny protokół łączności bezprzewodowe czujki systemu JABLOTRON mogą pracować do dwóch lat bez konieczności wymiany baterii (przy zastosowaniu baterii alkalicznych).

System JABLOTRON 100 umożliwia wydzielenie w systemie do 15 sekcji, które można załączać i wyłączać indywidualnie.

Fot. 2. Serwis zdalnej obsługi użytkownika

W każdej z nich można wyróżnić i zaprogramować nocny tryb pracy.

Oprócz urządzeń adresowalnych w systemie wykorzystuje się wyjścia nieadresowane, przeznaczone do sterowania automatyką i wskazywania stanów. Ze względu na potrzeby związane z automatyką zainstalowano 32 wyjścia, które można skonfigurować według potrzeby. Urządzenia sterujące tymi wyjściami mogą być bezpośrednio włączone do magistrali lub komunikować się z centralą drogą bezprzewodową. Przykładem wykorzystania takiego rozwiązania jest sterowanie bramą, która nie jest przyłączona przewodowo do systemu.

Wskaźniki i sygnalizatory informują światłem lub dźwiękiem o zaistniałym zdarzeniu. W celu przyśpieszenia i uproszczenia instalacji (krótszy czas i mniejsze koszty wykonania) zaprojektowano specjalne moduły na szynę DIN.

Uproszczenie obsługi uzyskano, nawiązując do logiki działania świateł drogowych, gdzie zielony kolor oznacza zezwolenie na przejście, a czerwony zabrania przejścia. W tym celu opracowano specjalne moduły sterowania, które są połączone z klawiaturą lub czytnikiem RFID. Każdy z nich ma przypisaną określoną funkcję. Na przykład pierwszy moduł załącza w dozór i wyłącza system w całym domu, drugi – tylko w garażu, a trzeci załącza światło. Jedyne, co musi zrobić użytkownik, aby zarządzać całością lub dowolną częścią systemu, to wcisnąć czerwony guzik na module w celu załączenia systemu lub sekcji w dozór lub zielony w celu wyłączenia tych sekcji z dozoru. Jeśli potrzebna jest autoryzacja, wystarczy, że użytkownik, po wciśnięciu guzika na module, przyłoży brelok lub kartę kontroli dostępu do czytnika RFID lub wpisze właściwy kod na klawiaturze. Po przydzieleniu odpowiednich uprawnień system umożliwia obsługę wielu urządzeń i sekcji z wykorzystaniem jedynie jednego breloka lub karty, albo jednego kodu. Użytkownik nie musi niczego szukać, wchodzić do menu systemu za pośrednictwem klawiatury, nie musi znać wielu haseł dostępu do poszczególnych funkcji. Dodatkowym atutem tego rozwiązania jest możliwość zdalnego dostępu poprzez stronę WWW. W tym przypadku użytkownik widzi na ekranie komputera lub telefonu graficzne odwzorowanie klawiatury zainstalowanej w domu. Logika obsługi zdalnej jest dokładnie taka sama. Na potrzeby łatwej obsługi zdalnej utworzono przeznaczony dla użytkowników systemów Jablotron Alarms serwis *www.jablonet.net*.

Artykuł ten ma na celu przybliżyć właściwości nowego systemu JABLOTRON 100. W kolejnych numerach zaprezentowane zostaną szczegółowe opisy dostępnych funkcji i możliwości konfiguracji.

Piotr Panek
Jablotron Alarms

MICRA

niezawodna ochrona małych obiektów

Część zleceń dla fachowca zajmującego się projektowaniem i realizacją zabezpieczeń dotyczy obiektów o niewielkich powierzchniach: warsztatów, sklepików, kiosków, garaży, domków letniskowych. W ich przypadku użycie standardowej centrali w celu zastosowania trzech czy czterech czujek mogłoby być ekonomicznie nieuzasadnione i niepotrzebnie skomplikowane. Właśnie dlatego powstał system MICRA. Moduł alarmowy MICRA, stanowiący serce systemu, ma funkcje prostej centrali alarmowej i komunikatora GSM/GPRS. Obsługiwanie zarówno standardowych czujek przewodowych, jak i przeznaczonych dla tego systemu czujek bezprzewodowych sprawia, że MICRA jest rozwiązaniem mającym wiele zastosowań

Podstawową cechą systemu MICRA, która odróżnia go od innych produktów dostępnych na rynku, jest prostota instalacji i konfiguracji. Moduł alarmowy MICRA jest wyposażony w zasilacz buforowy, odbiornik urządzeń bezprzewodowych 433 MHz oraz komunikator GSM/GPRS, które zazwyczaj są niedostępne w przypadku pojedynczego urządzenia. Oznacza to, że potrzebny jest tylko jeden kabel – do zasilania z sieci 230 V/50 Hz, a system MICRA można zainstalować w czasie krótszym niż godzina.

System MICRA jest łatwy w obsłudze. Jest obsługiwany głównie zdalnie, za pomocą pilotów. Można w nim zaprogramować do ośmiu pilotów. Przyciski każdego z nich mogą mieć indywidualnie przypisane funkcje. Pilota można używać nie tylko do załączania i wyłączania czuwania – może też służyć do wezwania pomocy (alarm napadowy) czy podnoszenia i opuszczania rolety przeciwwłamaniowej. Jeżeli jednak w konkretnej sytuacji lepszym rozwiązaniem będzie sterowanie przez wpisywanie kodów na wspólnej klawiaturze, można w tym celu wykorzystać bezprzewodową klawiaturę MKP-300. Zalety takiego rozwiązania można docenić m.in. w przypadku systemów, do których dostęp powinna mieć większa liczba użytkowników. Kolejnym sposobem obsługi systemu MICRA jest użycie telefonu komórkowego –zainicjowanie połączenia w celu identyfikacji numeru (wykorzystanie funkcji CLIP) i przesłanie lub odbiór sterowań przez telefon lub użycie komunikatów SMS. Niezależnie od wybranej metody obsługa jest bardzo intuicyjna, co ułatwia przeszkolenie końcowych użytkowników systemu.

Mimo iż MICRA jest przeznaczona do najmniejszych instalacji, może zapewnić wszechstronną ochronę obejmującą więcej niż tylko wykrywanie prób włamania. Firma SATEL oferuje bezprzewodowe czujki kontaktronowe MMD-300, bezprzewodowe czujki ruchu PIR MPD-300, które są odporne na zwierzęta, bezprzewodowe czujki zalania MFD-300 mogące ostrzec o zalaniu mieszkania wodą oraz czujki dymu i ciepła MSD-300 przeznaczone do wczesnego wykrywania pożaru. Aby jeszcze lepiej zabezpieczyć obiekt, do modułu MICRA można podłączyć do czterech standardowych czujek przewodowych. Zastosowanie urządzeń bezprzewodowych i przewodowych w jednym systemie zapewni maksymalną elastyczność w doborze jego wyposażenia.

Jedną z głównych zalet modułu MICRA jest zastosowanie efektywnego komunikatora GSM/GPRS, który umożliwia nie tylko przesyłanie informacji do stacji monitorującej, ale także powiadamianie za pośrednictwem CLIP/SMS o wybranych zdarzeniach oraz zdalne sterowanie systemem. Warto podkreślić, że właśnie takie zdalne sterowanie jest w tej klasie unikatowe – dotychczas

Fot. 1. Swoją wszechstronność moduł alarmowy MICRA zawdzięcza możliwości obsługi zarówno tradycyjnych czujek przewodowych, jak i dedykowanych czujek bezprzewodowych

Fot. 2. System MICRA to idealne rozwiązanie wszędzie tam, gdzie potrzebny jest prosty i niezawodny system alarmowy z komunikatorem GSM

Rys. 1. Wystarczy wysłać SMS lub zainicjować połączenie z numerem modułu MICRA (tzw. "CLIP"), aby załączyć lub wyłączyć czuwanie

było możliwe w przypadku zastosowania dużo droższych i bardziej skomplikowanych urządzeń.

Jeśli chcemy wykorzystać komunikator, wystarczy zainstalować w module kartę SIM dowolnego operatora GSM dostarczającego usługi w miejscu instalacji systemu. Moduł umożliwia zaprogramowanie do czterech numerów telefonu, na które wysyłane będą powiadomienia, oraz skonfigurowanie dwóch stacji monitorujących. Zdalne sterowanie jest możliwe za pośrednictwem SMS (wysyłanie do modułu wiadomości SMS o odpowiedniej treści) i z użyciem funkcji CLIP (zainicjowanie połączenia z odpowiedniego numeru).

Ciekawą funkcją modułu MICRA jest akustyczna weryfikacja alarmu. Dzięki zewnętrznemu mikrofonowi podłączonemu do modułu można usłyszeć, co dzieje się w chronionym obiekcie podczas alarmu, i na tej podstawie zdecydować, czy potrzebna jest interwencja.

Warto wiedzieć, że system MICRA może służyć nie tylko do zabezpieczenia przed włamaniem. Tryb modułu komunikacyjnego umożliwia dokonywanie pomiaru różnych wielkości fizycznych (temperatura, ciśnienie, obroty, poziom cieczy) reprezentowanych w postaci sygnałów napięciowych. Możliwe jest cykliczne raportowanie wyników pomiaru (telemetria) i reagowanie na przekroczenie zdefiniowanych uprzednio krytycznych wartości progowych (alarmy techniczne). Dzięki temu MICRA idealnie nadaje się do stosowania na stacjach pomp, w urządzeniach hydrotechnicznych czy elektrowniach wiatrowych jako moduł nadzorujący poprawność działania wyposażenia technicznego.

System MICRA może stanowić także tymczasowe zabezpieczenie obiektu, jeśli zaplanowane jest zastosowanie bardziej złożonego systemu lub sam obiekt ma charakter tymczasowy.

Wszystkich pragnących poznać pełnię możliwości systemu MICRA zapraszamy do udziału w praktycznych szkoleniach prowadzonych w ramach *Akademii SATEL*.

SATEL

Systemy alarmowe **Satel**

MICRA

bezprzewodowy system alarmowy

Niezawodna ochrona
dla małych obiektów

Bezprzewodowy system alarmowy MICRA jest idealnym rozwiązaniem wszędzie tam, gdzie potrzebny jest prosty i niezawodny system z komunikatorem GSM. Dzięki wykorzystaniu bezprzewodowych czujek, jego montaż jest szybki i niekłopotliwy. Obsługa za pomocą: pilotów, bezprzewodowego manipulatora czy telefonu komórkowego, jest prosta i intuicyjna. Dzięki wejściom analogowym, moduł alarmowy MICRA może pełnić także funkcję dozoru urządzeń technicznych przekazując informację o ich stanie, jak również o przekroczeniu krytycznych parametrów, np. temperatury lub ciśnienia.

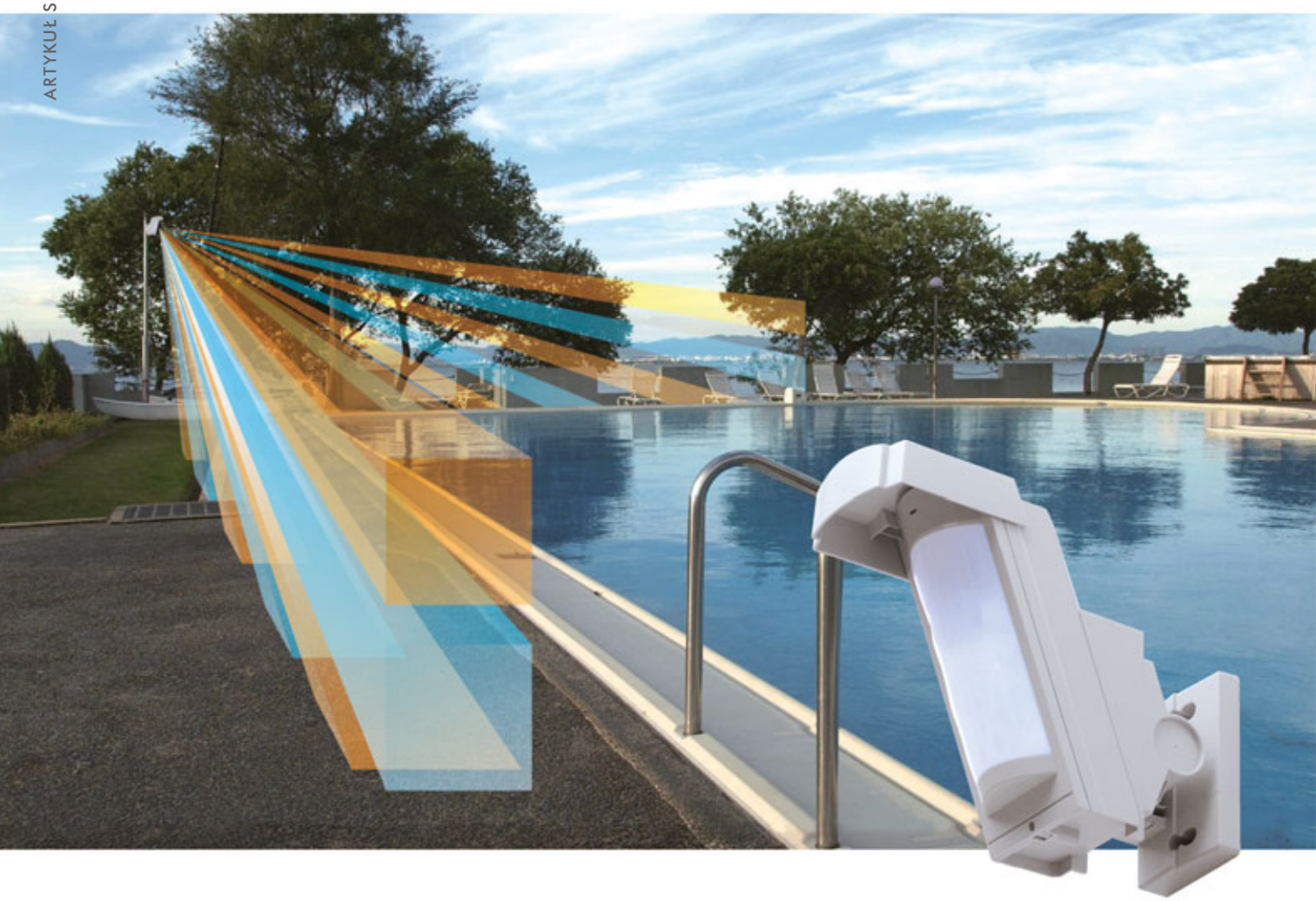
Prosty i szybki montaż, łatwa konfiguracja, intuicyjna obsługa i możliwość sterowania z telefonu komórkowego to główne zalety modułu MICRA.

Więcej informacji na
www.satel.pl

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

Satel

Czujki zewnętrzne serii HX
firmy OPTEX



Jarosław Gibas

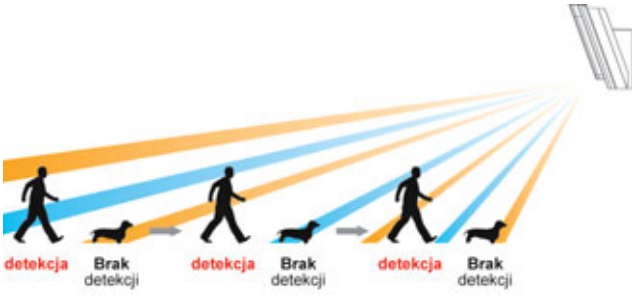
Firma OPTEX jest znana szerokiej rzeszy profesjonalistów ze swych wysokiej jakości czujek. Jako lider branży wyznacza kierunki rozwoju produktów i technologii służących wykrywaniu i przeciwdziałaniu włamaniom i ich skutkom. Będąc pionierem w tej dziedzinie, od wielu lat udoskonala produkty do ochrony zewnętrznej, których celem jest wykrycie intruza zanim zdoła on dokonać włamania. Celem zastosowania tego typu urządzeń jest uniknięcie szkód związanych z włamaniem dzięki odpowiednio wczesnemu wykryciu, zdemaskowaniu i odstraszeniu potencjalnego przestępcy. Jeśli nawet intruz nie wycofa się, ma znacznie mniej czasu na pozyskanie cennych zdobyczy i jest duża szansa na zatrzymanie go na gorącym uczynku przez odpowiednie służby. Korzyści z zastosowania szeroko rozumianej ochrony zewnętrznej są bezdyskusyjne, a koszty związane z jej zastosowaniem niewspółmiernie niskie w stosunku do potencjalnych strat spowodowanych włamaniem

Dla instalatora kwestie ochrony zewnętrznej są ważne tak samo jak dla właściciela obiektu. Instalacje zewnętrzne wymagają bowiem nie tylko specjalistycznej wiedzy, ale przede wszystkim zrozumienia mechanizmu detekcji i ograniczeń technologicznych, nieco doświadczenia oraz indywidualnego podejścia do każdej z nich. Pierwszy krok to identyfikacja potrzeb klienta oraz zagrożeń. Na tym etapie należy przeprowadzić precyzyjną analizę środowiska pracy czujek pod kątem potencjalnych źródeł fałszywych alarmów. Otwarta przestrzeń, światło słoneczne, zakres zmian temperatury, krzewy, drzewa, trawa, oczka wodne, zwierzęta – to wszystko ma istotny wpływ na pracę czujek zewnętrznych. Czujki zewnętrzne powinny wykorzystywać odpowiednie technologie i mieć odpowiednie funkcje, by można było sprawnie je zainstalować i dokonywać korekt potrzebnych z powodu wpływu wyżej wymienionych czynników środowiskowych. Skuteczność technologii i funkcji korygujących czujek jest uzależniona od jakości wstępnej analizy środowiskowej. Czujki serii HX były już tematem artykułu w prasie branżowej (Zabezpieczenia 5/2008), w którym skupiono się na technologiach i ich znaczeniu w kontekście stabilności pracy czujek w zmiennym środowisku zewnętrznym. Od tamtego czasu wprowadzono do oferty nowe modele czujek (np. czujkę dualną HX-40DAM) oraz serię czujek o charakterystyce kurtynowej (HX-80N). Powiększenie oferty jest na tyle istotne, że warto uporządkować wiedzę dotyczącą tych urządzeń.

Dostępne produkty

Seria czujek HX obejmuje produkty o dwóch charakterystykach pokrycia – kurtynowej (24 m×2 m) oraz przestrzennej (12 m×12 m). W przypadku obydwu wersji dostępne są modele standardowe (HX-40, HX-80N), z antymaskingiem (HX-40AM, HX-80NAM) oraz modele zasilane bateryjnie, przeznaczone do integracji z systemami bezprzewodowymi (HX-40RAM, HX-80NRAM). Czujka dualna z antymaskingiem (HX-40DAM) jest dostępna tylko w wersji z charakterystyką przestrzenną (12 m×12 m).

O jakości systemu alarmowego świadczy zdolność do wykrycia intruza oraz liczba tzw. fałszywych alarmów, czyli aktywacji systemu w sytuacji, gdy na chronionym obszarze nie ma intruza. Czujki HX pracują stabilnie w bardzo różnych warunkach środowiskowych, wychwytując intruza w nawet najbardziej niesprzyjających okolicznościach. Skuteczność wyszukanych technologii zależy w wysokim stopniu od instalatora, który powinien najpierw ocenić środowisko pracy czujki, a potem zainstalować ją w odpowiednim miejscu. Czujki HX są łatwe do zainstalowania. Wszystkie akcesoria potrzebne do montażu i ewentualnego strojenia są dostarczane wraz z czujką w jednym pudełku. Instalator powinien oczywiście posiadać odpowiednie narzędzia oraz zaopatrzyć się w akcesoria montażowe (kołki, kotwy, wkręty itp.) dostosowane do podłoża, do którego należy przymocować urządzenie. Pudełko zawiera szablony montażowe ułatwiające pracę na wysokości. Wraz z czujką dostarczany jest również daszek, który zabezpiecza czujkę przed „oślepieniem" przez słońce, i wspornik montażowy, który umożliwia obrócenie jej o ±90° oraz pochylenie o ±20°. Należy



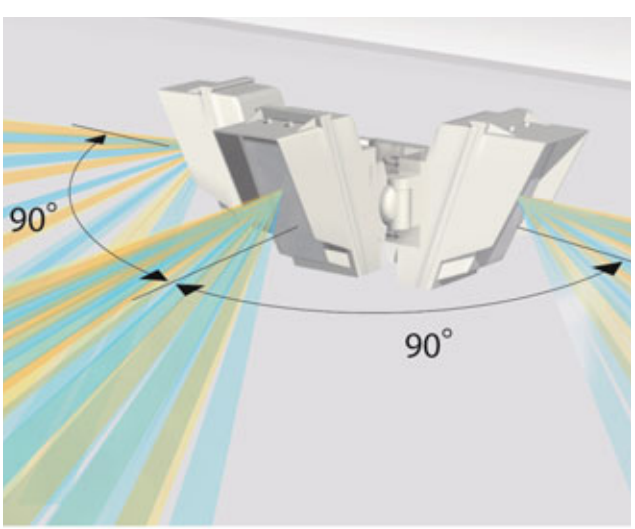
Rys. 1. Inteligentny algorytm detekcji czujek HX

pamiętać, że ze względu na wyszukane algorytmy analizy, które są ściśle związane z rozkładem geometrycznym pól detekcji, pochylenie czujki ma na celu wyłącznie kompensację nachylenia podłoża. Przestrzeganie tej zasady jest niezwykle istotne i ma na celu uzyskanie wysokiej jakości pracy urządzenia.

Z długoletnich doświadczeń firm oferujących ochronę zewnętrzną wynika, że częstą przyczyną występowania fałszywych alarmów jest zbyt rozległe pole widzenia czujki, wykraczające poza obszar, który powinien być obserwowany. Równie częstą przyczyną jest aktywność małych zwierząt w polu widzenia czujki bądź insektów, które dostały się do jej wnętrza. Działanie urządzenia mogą zakłócać również kołyszące się na wietrze drzewa, krzewy itp.

Techniki zwiększające stabilność pracy

Stabilność działania czujki można poprawić, ograniczając pole jej widzenia. Istniejące rozwiązania, np. redukcja czułości, są nieadekwatne do oczekiwań, ponieważ ograniczają wykrywalność intruzów. Jak dotąd najlepszym rozwiązaniem jest zamaskowanie odpowiednich pól soczewki, które powoduje zawężenie strefy detekcji i wykluczenie z niej obiektów, które mogą powodować fałszywe alarmy. Dokładny wykres pola detekcji znajdujący się w instrukcji oraz dostarczone wraz z czujką naklejki maskujące pozwalają sprawnie i precyzyjnie ograniczyć pole detekcji. Również czujnik mikrofalowy w czujce HX-40DAM umożliwia skuteczne ograniczenie pola detekcji przez dwustopniową regulację zasięgu – skokowo (przełącznikiem) oraz bezstopniowo (pokrętłem)



Rys. 2. Uchwyt montażowy z zestawu serii HX daje dużą swobodę wyboru miejsca instalacji

– co jest istotnym uzupełnieniem funkcjonalności kanałów detekcji PCP. Dzięki temu można zainstalować więcej czujek w niedużej odległości od siebie. Czujka kurtynowa (HX-80N) umożliwia ograniczenie długości kurtyny oraz niezależnie strefy bezpośrednio pod czujką. Zwiększa to swobodę wyboru miejsca instalacji czujki.

Wpływ przemieszczania się małych zwierząt na obszarze ochronionym na działanie czujki ograniczają również zaawansowane metody analizy sygnałów oraz wyszukane połączenie optyki oraz algorytmów analizy danych. Geometryczny rozkład pól czułości obydwu kanałów PCP oraz odległość pomiędzy poszczególnymi warstwami powodują, że zastosowane algorytmy umożliwiają analityczne rozróżnienie sygnałów generowanych przez człowieka i małe zwierzęta. Ponadto technologia ta pozwala na wykrycie intruza zmierzającego wprost do czujki znacznie skuteczniej niż klasyczne rozwiązania. Aby w pełni wykorzystać udogodnienia technologiczne, wystarczy przestrzegać podstawowych zasad instalacji czujki dotyczących wysokości jej montażu i pochylenia.

Wpływ roślinności na pracę czujek jest najczęściej kojarzony z działaniem wiatru. Przemieszczanie się mas powietrza nie powoduje istotnych zmian w obrazie termicznym otoczenia, co nie powoduje bezpośrednio zadziałania czujki. Czujka PCP jest aktywowana przez cykliczne odsłanianie miejsc zacienionych (zimniejszych) przez kołyszące się rośliny. O ile jesteśmy w stanie skutecznie wyeliminować to źródło fałszywych alarmów przez maskowanie pojedynczej rośliny (krzewy), o tyle nie możemy zastosować tej metody w przypadku wysokiej trawy. Tu potrzeba czegoś bardziej wyszukanego – analitycznej metody filtrowania sygnałów. Spektralna analiza sygnałów pozwala oddzielić składowe sygnału wywołanego przez poruszające się na wietrze rośliny ze względu na ich charakterystyczne cechy (np. powtarzalność) i w ten sposób eliminować potencjalne fałszywe alarmy, zwiększając stabilność pracy czujki.

Podsumowanie

Z punktu widzenia instalatora łatwość korzystania z tych udogodnień oraz dostępność wszystkich przełączników zaraz po otwarciu jej obudowy daje duży komfort pracy i umożliwia szybkie i łatwe korygowanie ustawień z maskowaniem pola detekcji włącznie. Stopień ochrony IP55 oraz dodatkowe uszczelnienia przepustów kablowych chronią wnętrze czujki przed brudem, pyłem oraz penetrowaniem obudowy przez insekty (szczególnie wiosną), co wymusza kosztowne, niezaplanowane wizyty serwisowe.

Podsumowując – czujki zewnętrzne OPTEX, zwłaszcza z serii HX, wyznaczają zupełnie nowe standardy technologii detekcji, eliminowania fałszywych alarmów i funkcji wspierających pracę instalatora. Łatwy dostęp do istotnych elementów czujki i zdolność modelowania/maskowania obszaru detekcji bez zmiany czułości lub innych właściwości zwiększa stabilność pracy urządzenia oraz wykrywalność niezależnie od warunków środowiskowych.

Jarosław Gibas
Optex Security

ZASIĘG
AŻ DO 240
METRÓW

TECHNOLOGIA LED SMD

ŻYWOTNOŚĆ: 11 LAT

WYDAJNOŚĆ: +20%

OSZCZĘDNOŚĆ ENERGII

NISKIE KOSZTY

5 LAT GWARANCJI

GEKO PEŁNA GAMA OŚWIETLACZY LED

Linia GEKO reaguje na wymagania doskonałego oświetlenia zapewniającego wyraźny obraz CCTV w warunkach nocnych. Zastosowaliśmy w urządzeniach najwyższej jakości komponenty, a ich innowacyjną architekturę zaprojektowaliśmy ze szczególną starannością. Dlatego możemy dać pełną gwarancję na optymalne osiągi, wysoką wydajność, maksymalną trwałość oraz niskie koszty naszych oświetlaczy.

VIDEOTEC

Nowe spojrzenie
na ochronę informacji niejawnych (cz. 2)

Artur Bogusz

Kontynuując rozpoczęty cykl rozważań dotyczących ochrony informacji niejawnych, poruszę kwestię ochrony informacji w firmach w świetle uwarunkowań prawnych nowej ustawy o ochronie informacji niejawnych. Niniejsza część dotyczy głównie problemu funkcjonowania pionu ochrony informacji niejawnych w przedsiębiorstwach. Zagadnienia uzyskania i wykorzystywania świadectwa bezpieczeństwa przemysłowego będą opisane w kolejnej części

Omawiając w poprzednim artykule (*Zabezpieczenia* nr 3/2012) rolę państwa w ochronie informacji niejawnej oraz kwestie identyfikacji, klauzulowania i nadzorowania informacji, skupiłem się głównie na wymogach prawnych oraz oddziaływaniu nadzorczym z zewnątrz instytucji/firmy/przedsiębiorstwa. Ustawodawca określił także działania wewnątrz firmy, czyli zobowiązania przedsiębiorcy[1] – kierownika przedsiębiorcy[2], traktowanego w myśl przepisów ustawy jako kierownika jednostki organizacyjnej[3] (KJO), dając zarazem wykładnię tego pojęcia oraz specyfikując listę osób wykonujących obowiązki KJO (obejmującą likwidatora oraz syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym).

1. Obowiązki kierownika jednostki organizacyjnej w zakresie ochrony informacji niejawnych

Pragnę podkreślić, że opisywane w dalszej części artykułu zagadnienia dotyczą wyłącznie ochrony informacji niejawnych zgodnych z wymaganiami przywołanej ustawy – tzn. wyodrębnionych i zidentyfikowanych (klauzula i oznakowanie), odpowiednio przechowywanych i udostępnianych (uprawnienia użytkowników), przetwarzanych w określony sposób (wg szczególnych wymagań bezpieczeństwa – SWB i procedur bezpiecznej eksploatacji – PBE)[4].

Przypominam o tym ze względu na spotykane w mojej praktyce zawodowej częste pomyłki prawne. Na przykład tajemnica przedsiębiorcy/przedsiębiorstwa, zapisana w postaci notatki czy też protokołu z posiedzenia zarządu spółki, zostaje oznakowana klauzulą „poufne" lub nawet „tajne", mimo iż nie spełnia przywołanych w ustawie wymagań formalnych, tymczasem w kwestii tajemnicy przedsiębiorstwa podstawowym aktem prawnym jest art. 39 ust. 2 umowy międzynarodowej – Porozumienia TRIPS (obowiązującego w Polsce od 1.01.2000)[5]. Zgodnie z tym przepisem „osoby fizyczne i prawne będą miały możliwość zapobiegania, aby informacje pozostające w sposób zgodny z prawem pod ich kontrolą nie zostały ujawnione, nabyte lub użyte bez ich zgody przez innych, w sposób sprzeczny z uczciwymi praktykami handlowymi, jak długo takie informacje są poufne (w sensie ograniczonej dostępności) i mając wartość handlową są poddane rozsądnym, w danych okolicznościach, działaniom dla utrzymania ich poufności". Przepis ten ma charakter samowykonalny (*self-executing*), co oznacza, że przedsiębiorca może się powołać na niego bezpośrednio. Jego rozszerzeniem użytkowym są zapisy ustawy o zwalczaniu nieuczciwej konkurencji[6] oraz rozwiązania dotyczące informacji chronionej, które wynikają z kodeksów (karnego, cywilnego i spółek handlowych) i dotyczą tajemnic służbowych, gospodarczych, organizacyjnych, technicznych i technologicznych.

Pragnę przypomnieć po raz kolejny, że tylko informacje niejawne wydzielone w odrębnym zasobie i odpowiednio oznakowane (klauzule – patrz: artykuł cz. 1, podpunkt 3.1), przetwarzane, przechowywane oraz chronione, są objęte wymaganiami przedmiotowej ustawy. Zakres ujętej w ustawie odpowiedzialności zarządczej przedstawia rysunek nr 1.

1.1. Szczególne wymagania ustawowe wobec KJO

Ustawodawca nakłada na KJO obowiązek ochrony informacji niejawnych na terytorium przez niego zarządzanym

1) Art. 2 pkt 13 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228), z odwołaniem do art. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (tekst jednolity: Dz. U. z 2007 r., nr 155, poz. 1095 z późn. zm.).

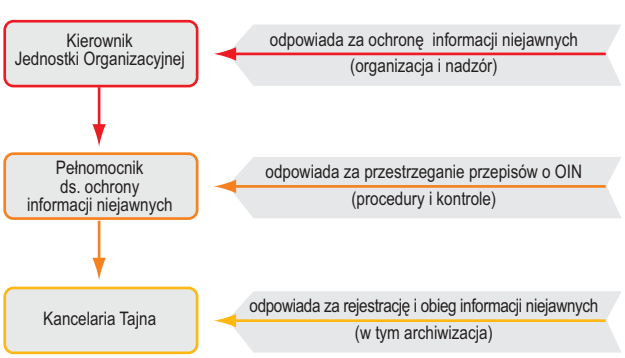
2) Art. 2 pkt 14) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

3) ibidem

4) Art. 8 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

5) Porozumienie w sprawie handlowych aspektów praw własności intelektualnej ("Agrement on Trade – Related Aspects of Intellectual Property Rights"), zał. do Dz. U. z 1996 r., nr 32, poz. 143.

6) Art. 11, ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity: Dz. U. z 2003 r., nr 153, poz. 1503 z późn. zm.).



Rys. 1. Odpowiedzialność w systemie ochrony informacji niejawnych firmy

Rys. 2. Kontrola ochrony informacji niejawnych w firmie

(w instytucji/firmie/przedsiębiorstwie)[7], we wszystkich aspektach nadzoru, z zachowaniem podstawowych atrybutów, tzn. poufności, integralności i dostępności. W praktyce jest to związane ze zorganizowaniem ochrony (pion ochrony) oraz zapewnieniem jej poprawnego funkcjonowania w firmie (ludzie, pieniądze, pomieszczenia i niezbędne urządzenia). Kierownik jednostki organizacyjnej może przekazać swoje obowiązki i związane z nimi uprawnienia wybranej osobie, ale nie dotyczy to jego ustawowego obowiązku odpowiedzialności za ochronę informacji niejawnych z racji formalnego nakazu jej organizowania i stałego nadzorowania, za którego realizację ponosi pełną odpowiedzialność (szczególnie dotyczy to czynności zarządczych z zakresu OIN wyszczególnionych w ustawie[8]).

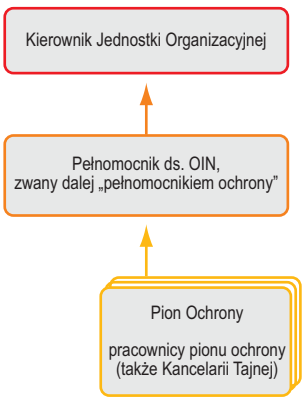
Schematycznie oddziaływania kontrolno-nadzorcze na obszar ochrony informacji niejawnych w firmie przedstawione są na rysunku nr 2.

1.2. Realizacja ochrony informacji niejawnych w firmie

KJO ma do dyspozycji zatrudnionego przez siebie pełnomocnika do spraw ochrony informacji niejawnych oraz powoływany (jeśli jest taka potrzeba) pion ochrony informacji niejawnych (podobnie jak w przypadku innych, wyspecjalizowanych czynności zarządczych/rozliczeniowych).

W celu przetwarzania informacji o klauzulach „tajne" lub „ściśle tajne" KJO ma obowiązek utworzenia kancelarii tajnej[9] jako odrębnej komórki organizacyjnej odpowiedzialnej za rejestrowanie i obieg dokumentacji niejawnej oraz zatrudnienie jej kierownika. W art. 8 omawianej ustawy ustawodawca jednoznacznie podał, że informacje niejawne, którym nadano określoną klauzulę tajności:

- mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do informacji o określonej klauzuli tajności;
- muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;
- muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.



Rys. 3. Organizacja systemu ochrony informacji niejawnych

Ustawa i rozporządzenia wykonawcze[10] nie pozostawiają żadnych wątpliwości – dozwolone jest wyłącznie postępowanie zgodne z zapisami w opublikowanych dokumentach, a wszelkie inne działania są zabronione pod rygorem odpowiedzialności karnej.

2. Pion ochrony informacji niejawnych w firmie

Ochrona informacji niejawnych wymaga szeregu procedur (zakres nadzoru jest przedstawiony na rysunku nr 1) realizowanych przez odpowiednio sprawdzone i przeszkolone osoby, które są zebrane w komórce organizacyjnej zwanej pionem ochrony informacji niejawnych (POIN). Skład osobowy POIN obejmuje:

- pełnomocnika do spraw ochrony informacji niejawnych (OIN) oraz jego zastępcę/zastępców (o ile zostali wyznaczeni);
- inspektora bezpieczeństwa teleinformatycznego (BTI) – w przypadku posiadania systemu/systemów teleinformatycznych (TI) do przetwarzania informacji niejawnych (wg wymogów SWB i PBE);
- kierownika kancelarii tajnej i jej personel (dotyczy to filii lub podkancelarii, o ile istnieją).

Ponadto powoływana jest osoba (lub zespół osób) nie będąca inspektorem BTI, zwana administratorem systemu (o odpowiednich uprawnieniach), odpowiedzialna za funkcjonowanie niejawnego systemu TI oraz przestrzeganie zasad i wymagań dotyczących bezpieczeństwa.

W większości przypadków ów pion ochrony, o którym tak szumnie pisze się w ustawie, to jedna osoba (pełnomocnik ds. ochrony). Kierownika kancelarii tajnej nie biorę tu pod uwagę, gdyż jego zadania są jasno określone i dotyczą funkcjonowania właśnie kancelarii tajnej. Wynika z tego jasno, że wymienione i wskazane w ustawie wszystkie obowiązki pełnomocnik ds. ochrony realizuje zupełnie sam. Biorąc pod uwagę dość złożoną sytuację pełnomocników ds. ochrony w Polsce i to, że bardzo często wypełniają oni swoje obowiązki w więcej niż dwóch jednostkach organizacyjnych w tym samym czasie, nietrudno sobie wyobrazić, jaka jest jakość ich pracy.

Może się również zdarzyć, że przedsiębiorstwo nie posiada pionu ochrony ani kancelarii tajnej, gdyż w przypadku przedsiębiorstwa prowadzonego przez jedną osobę zdolność

7) Art. 14 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

8) Art. 13, ust. 1 – współdziałanie ze służbami; art. 14, ust. 2 – zatrudnienie pełnomocnika; art. 48, ust. 9 – akredytacja STI „Zastrzeżone"; art. 49, ust. 5 – opracowanie SWBS i PBE; art. 52, ust. 1, pkt 1 – wyznaczanie inspektora BTI; art. 52 ust. 1, pkt 2 – wyznaczanie administratora niejawnego STI; art. 56 ust. 1 – wnioskowanie o ŚBP; art. 71 ust. 3 – wyznaczenie osoby odpowiedzialnej za OIN wg zawartej umowy.

9) Art. 42, ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

10) Zestawienie obowiązujących rozporządzeń znajduje się w podpunkcie 6.2 niniejszego artykułu.

do ochrony informacji niejawnych jest potwierdzana poświadczeniem dotyczącym ich bezpieczeństwa, upoważniającym do dostępu do informacji niejawnych o klauzuli tajności „poufne" lub wyższej, które jest wydawane przez ABW albo SKW, i zaświadczeniem o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych wydawanym przez ABW albo SKW[11]. W takim przypadku istnieją jednak określone w rozporządzeniach wykonawczych ustawy ograniczenia, a przedsiębiorca ponosi wszelkie konsekwencje niewypełnienia swoich obowiązków.

2.1. Pełnomocnik ochrony informacji niejawnych

Pełnomocnikiem ochrony informacji niejawnych – IN (nazwa w brzmieniu ustawowym) może być osoba, która posiada:
- obywatelstwo polskie,
- wykształcenie wyższe,
- odpowiednie poświadczenie bezpieczeństwa wydane przez ABW albo SKW, a także przez były Urząd Ochrony Państwa lub byłe Wojskowe Służby Informacyjne,
- zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW albo SKW, a także przez byłe Wojskowe Służby Informacyjne.

Zwracam uwagę na konieczność posiadania wykształcenia wyższego przez pełnomocnika ochrony IN (obowiązuje to od 1 stycznia 2011 roku).

Kierownik jednostki organizacyjnej może zatrudnić zastępcę lub zastępców pełnomocnika ochrony IN (z zastrzeżeniem spełnienia przez te osoby warunków, o których mowa wyżej). Szczegółowy zakres obowiązków zastępcy pełnomocnika ochrony IN określa kierownik jednostki organizacyjnej. Bardzo często funkcja zastępcy pełnomocnika jest traktowana przez potencjalnych pracodawców jako metoda zdobycia kolejnych środków na zatrudnienie w pionie ochrony kolejnej osoby. Kiedy jednak pojawia się problem nagłej i nieprzewidzianej nieobecności pełnomocnika ochrony, który pełni funkcję sam, a zorganizowany przez niego system ochrony informacji niejawnych jest systemem nie dającym się odtworzyć podczas jego nieobecności, pojawia się problem. Kiedy okazuje się, że jest możliwość wskazania zastępcy pełnomocnika, zastanawiają się, dlaczego z tego praktycznego wyjścia nie skorzystali.

Chciałbym przypomnieć kierownikom jednostek organizacyjnych, że pełnomocnik ochrony IN, wypełniając obowiązki wymienione w ustawie, jest w stanie właściwie zabezpieczyć informacje niejawne w jednostce organizacyjnej. Kierownik jednostki organizacyjnej powinien zapewnić pełnomocnikowi właściwy warsztat pracy i umożliwić mu wypełnianie ustawowych obowiązków.

2.1.1. Zadania pełnomocnika ochrony IN

Do ustawowych zadań pełnomocnika ochrony IN należy:
- zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego,
- zapewnienie ochrony systemów teleinformatycznych, w których przetwarzane są informacje niejawne,
- zarządzanie ryzykiem ujawnienia informacji niejawnych, w szczególności szacowanie ryzyka,
- kontrola ochrony informacji niejawnych oraz przestrzegania przepisów dotyczących ochrony tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów,
- opracowywanie i aktualizowanie wymagającego akceptacji kierownika jednostki organizacyjnej planu ochrony informacji niejawnych w jednostce organizacyjnej, także w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji,
- prowadzenie szkoleń w zakresie ochrony informacji niejawnych,
- prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających,
- prowadzenie aktualnego wykazu osób zatrudnionych, pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto,
- przekazywanie (odpowiednio ABW lub SKW, o których mowa w art. 73 ust. 1 ustawy) do ewidencji danych (o których mowa w art. 73 ust. 2 tejże ustawy) osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub osób, których poświadczenie bezpieczeństwa cofnięto na podstawie prowadzonego wykazu.

Ponadto kierownik jednostki organizacyjnej może powierzyć pełnomocnikowi ochrony IN oraz pracownikom pionu ochrony wykonywanie innych zadań, jeżeli nie zakłóci to wypełniania obowiązków ustawowych, o których była mowa wyżej. W Polsce pełnomocnicy ochrony IN w jednostkach organizacyjnych są zazwyczaj obciążani wszystkimi dodatkowymi obowiązkami powiązanymi mniej lub bardziej z bezpieczeństwem. Odpowiadają za zabezpieczenia techniczne, fizyczne, informatyczne czy bezpieczeństwo osób. Jeżeli zakres ich obowiązków nie wyklucza obarczenia ich dodatkowymi zadaniami, to nie ma problemu. Niestety w praktyce odbywa się to kosztem jakości ich pracy.

2.1.2. Zadania pracownika ochrony

Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która posiada:
- obywatelstwo polskie (nie dotyczy to pracowników pionu ochrony zatrudnionych u przedsiębiorców),
- odpowiednie poświadczenie bezpieczeństwa lub upoważnienie, o którym mowa w art. 21 ust. 4 pkt 1 ustawy,
- zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych.

I znowu nasza praktyka dostosowywania się do przepisów ustawy o ochronie informacji niejawnych pokazuje, że bardzo rzadko w jednostkach organizacyjnych uzupełnia się pion ochrony dodatkowymi pracownikami, którzy mogą realizować wszelkie niezbędne z punktu widzenia ustawy zadania. Głównym ich działaniem byłoby wspomaganie pełnomocnika

11) Art. 54 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

ochrony IN z naciskiem na wykonywanie zadań pionu ochrony wynikających z ustawy.

2.1.3. Praktyka funkcjonowania pionu ochrony informacji niejawnych

W dobie powszechnego oszczędzania trudno sobie wyobrazić piony ochrony, w których każdy pracownik ma tylko jeden obowiązek i nie wykonuje żadnych innych zadań. Niemniej równie trudno, a być może trudniej, wyobrazić sobie funkcjonowanie pionu ochrony informacji niejawnych w jednostce organizacyjnej, w której wszystkie obowiązki spoczywają na jednym pracowniku – pełnomocniku ochrony IN, a jednak jest to zjawisko nagminne i dlatego tak często piony te nie funkcjonują poprawnie. Według mnie (a moja ocena wynika z wieloletniej praktyki) w większości przypadków działanie jednoosobowych pionów ochrony jest po prostu nieskuteczne. Wszyscy właściciele firm, prezesi, dyrektorzy, a więc – innymi słowy – kierownicy jednostek organizacyjnych, w których pion jest jednoosobowy, powinni zadać sobie pytanie: czy w mojej jednostce organizacyjnej prawidłowo zabezpiecza się informacje niejawne?

2.1.4. Reakcje na naruszenia

W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów dotyczących ochrony informacji niejawnych pełnomocnik ds. ochrony zawiadamia kierownika jednostki organizacyjnej i niezwłocznie podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków. W przypadku stwierdzenia naruszenia przepisów dotyczących ochrony informacji niejawnych o klauzuli „poufne" lub wyższej pełnomocnik ds. ochrony zawiadamia niezwłocznie również ABW albo SKW. Pełnomocnik ochrony IN ma obowiązek powiadomić ABW albo SKW także wówczas, gdy przepisy dotyczące ochrony informacji niejawnych zostaną naruszone przez kierownika jednostki organizacyjnej.

2.2. Ochrona informacji niejawnych – obowiązujące regulacje prawne

Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 roku dokonała w swoim tekście zmian w 107 innych dokumentach ustanawiających przepisy prawa w RP (prawach wydanych z mocą ustawową, kodeksach prawa, ustawach) odwołując się w swej treści do kilkunastu obowiązujących aktów prawa oraz nakazując wydanie przepisów szczegółowych (rozporządzenia okołostawowe), dając w tym zakresie delegacje wykonawcze Prezesowi Rady Ministrów i poszczególnym ministrom.

Zgodnie z zasadą obowiązywania ogłoszonych norm konieczność zapoznania się z dokumentami prawa stanowionego (ustawami, rozporządzeniami) jest wymagana, a nieznajomość przepisów nie zwalnia od odpowiedzialności za skutki ich nieprzestrzegania, co powinni wziąć pod uwagę wszyscy KJO.

Na dzień 1 stycznia 2012 roku obowiązywały nw. rozporządzenia wykonawcze dotyczące ochrony informacji (wymieniam w kolejności ich ogłaszania):

- Dz. U. z 2010 r., nr 258, poz. 1751 – dot. szkolenia z zakresu ochrony informacji niejawnych;
- Dz. U. z 2010 r., nr 258, poz. 1752 – dot. poświadczeń bezpieczeństwa osobowego;
- Dz. U. z 2011 r., nr 67, poz. 356 – dot. opłat za sprawdzanie bezpieczeństwa przemysłowego;
- Dz. U. z 2011 r., nr 86, poz. 470 – dot. wzorów dokumentów mających związek z bezpieczeństwem przemysłowym;
- Dz. U. z 2011 r., nr 93, poz. 541 – dot. kontroli ochrony informacji niejawnych;
- Dz. U. z 2011 r., nr 156, poz. 26 – dot. zasad akredytacji systemów teleinformatycznych przeznaczonych do przetwarzania i ochrony informacji niejawnych (BTI OIN);
- Dz. U. z 2011 r., nr 159, poz. 948 – dot. wymagań odnoszących się do bezpieczeństwa teleinformatycznego informacji niejawnych;
- Dz. U. z 2011 r., nr 159, poz. 949 – dot. opłat za kontrolę bezpieczeństwa teleinformatycznego;
- Dz. U. z 2011 r., nr 220, poz. 1302 – dot. ustanowienia Krajowej Władzy Bezpieczeństwa w kontaktach międzynarodowych (współdziałanie ABW i SKW);
- Dz. U. z 2011 r., nr 271, poz. 1603 – dot. przewozu dokumentów mających związek z ochroną informacji niejawnych;
- Dz. U. z 2011 r., nr 276, poz. 1631 – dot. organizacji kancelarii tajnych;
- Dz. U. z 2011 r., nr 288, poz. 1692 – dot. oznaczania dokumentów zawierających informacje niejawne oraz sposobu zmiany ich wcześniejszych klauzul;

Pominąłem tutaj rozporządzenia resortowe oraz dokumenty publikowane w dziennikach urzędowych poszczególnych ministrów, jednak zachęcam do zapoznania się z ich treścią.

Artur Bogusz

Bibliografia

1. Anzel M., *Nowa ustawa i jej zmienione uwarunkowania*, mat. szkoleniowe OSPOIN, Warszawa 2010.
2. Hoc St., *Ustawa o ochronie informacji niejawnych. Komentarz*, wyd. LexisNexis, Warszawa 2010.
3. Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, wyd. LexisNexis, Warszawa 2011.
4. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych, Dz. U. z 2010 r., nr 182, poz. 1228.
5. *Wytyczne w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne*, zał. do *Decyzji nr 362/MON* z dnia 28 września 2011 r.

Security Products SINCE 1991 roger

seria radius

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.
- **INTEGRACJA** z innymi systemami:

RCP CCTV SSWiN

RCP Master *PR602LCD*

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

roger®

www.roger.pl

Wprowadzono do oferty **PR102DR**
- nowy, ekonomiczny kontroler dostępu zasilany z 12VDC

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

NOVUS MANAGEMENT SYSTEM

Profesjonalne oprogramowanie do monitoringu wizyjnego IP

NMS - NOVUS MANAGEMENT SYSTEM należy do rodziny produktów NOVUS IP

Wszystkie produkty w ramach tej serii są ze sobą kompatybilne i pozwalają tworzyć rozbudowane systemy monitoringu wizyjnego po sieciach TCP/IP z rozproszonymi centrami rejestracji i nadzoru, skupiającymi wiele spersonalizowanych stanowisk operatorskich.

Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Dlaczego oprogramowanie

NOVUS MANAGEMENT SYSTEM

✓**program jest bezpłatny**
dostaniesz go w komplecie kupując urządzenie IP marki NOVUS®

✓**nie ponosisz żadnych dodatkowych kosztów, gdy chcesz rozbudować system**
NMS nie ma ograniczeń licencyjnych co do liczby podłączonych urządzeń, liczby użytkowników i pojemności dysków, umożliwia tworzenie systemów rozbudowanych nawet do kilkuset kamer

✓**możesz rejestrować do 64 strumieni wideo w rozdzielczości HD na jednej stacji roboczej**
nie musisz rezygnować z wysokiej jakości nagrań i w pełni wykorzystujesz możliwości kamer megapikselowych

✓**program jest łatwy w obsłudze**
ma intuicyjny interfejs graficzny, umożliwia pracę wielomonitorową i tworzenie własnych układów paneli roboczych

✓**możesz zintegrować system CCTV z systemem SSWiN marki DSC**
łatwiej zarządzasz bezpieczeństwem obiektu

✓**sterujesz kamerami PTZ z poziomu aplikacji oraz za pomocą klawiatury z dżojstikiem**
obsługa kamer PTZ jest tak wygodna, jak sterowanie kamerami analogowymi

✓**w zależności od wielkości systemu wybierasz wariant oprogramowania dostosowany do potrzeb konkretnej instalacji**
- do dużych, rozbudowanych systemów, zalecana jest instalacja **oprogramowania w wersji wielostanowiskowej** - Klient (wyświetlanie) + Serwer (nagrywanie). Takie rozwiązanie pozwala na bezobsługową pracę jednostki serwerowej oraz podnosi bezpieczeństwo i stabilność systemu
- do małych systemów zalecana jest instalacja **oprogramowania w wersji jednostanowiskowej** - Klient/Serwer (nagrywanie i wyświetlanie)

Więcej informacji o oprogramowaniu NMS oraz wersję demo znajdziesz na

www.nmsip.pl

Krzysztof Białek

Socjotechnika

Wielu z nas żyje w przekonaniu, że haker to komputerowy maniak, wyobcowany, przyrośnięty do klawiatury dziwak, który przez swoje skłonności do wielogodzinnego przesiadywania przed ekranem komputera nie jest przystosowany do życia w społeczeństwie. Myślimy, że takiemu człowiekowi trudno znaleźć nić porozumienia ze zwykłymi ludźmi, ponieważ posługuje się językiem zrozumiałym tylko dla wytrawnych informatyków. Czy tak jest na pewno? Nie zawsze… Hakerem nazywana jest osoba, która przełamuje zabezpieczenia systemów informatycznych, wykorzystując luki, które się w nich znajdują, atakuje systemy informatyczne za pośrednictwem specjalnego oprogramowania. Hakerem jest również osoba, która posiada wyjątkowe umiejętności interpersonalne, zdolność do manipulowania ludźmi, co w połączeniu z wiedzą informatyczną daje wybuchową mieszankę

Dziś informacja jest największą wartością. Im bardziej krytyczna, ukrywana, tym cenniejsza. Niewielu z nas zdaje sobie sprawę z faktu, iż wiele informacji mało istotnych z naszego punktu widzenia, czy z punktu widzenia pracowników naszej firmy, może stanowić wielką wartość dla kogoś z zewnątrz. Sposobów na pozyskanie cennych informacji może być wiele, a dodatkowym kłopotem jest to, iż ustalenie przyczyny wycieku informacji może być bardzo trudne. O ile utrata pieniędzy zostanie zauważona prędzej czy później, o tyle źródła wycieku możemy nie ustalić nigdy. Przestępcy mogą zdobyć interesujące ich informacje, włamując się do mieszkania czy biura. Efekty zwykłego włamania widać od razu. Trudniej natomiast zorientować się, że ktoś włamał się do systemu operacyjnego komputera. Najtrudniej jednak zorientować się, w jaki sposób przestępca zdobył wartościowe informacje wtedy, gdy sami spowodowaliśmy ich wyciek.

„Standardowo" hakerzy atakują zabezpieczenia bezdusznych systemów komputerowych, natomiast hakerzy-socjotechnicy atakują najsłabsze ogniwo wszystkich systemów – człowieka. Jedni ludzie są bardziej podatni na tego rodzaju ataki, inni mniej. Aby móc poradzić sobie z tego rodzaju zagrożeniami, trzeba po prostu zdawać sobie sprawę z faktu, iż możemy stać się celami ataku, i zachować czujność oraz zdrowy rozsądek. Jakie metody wykorzystują socjotechnicy, aby wejść w posiadanie cennych dla nich informacji? Przeróżne. Kilka z nich postaram się pokrótce opisać.

Jedną z metod wyłudzania poufnych informacji jest phishing. Proceder ten był już szerzej opisywany na łamach naszego periodyku, dlatego opiszę go tylko pobieżnie. Można go porównać do strzelania ze śrutówki bez celowania, byleby w kierunku stada kaczek przelatujących nad głową, z nadzieją, że na drodze wystrzelonego pocisku znajdzie się przypadkowa kaczka. Celem phishingu, najczęściej w postaci spamu (spreparowanych wiadomości automatycznie wysyłanych na przypadkowe adresy e-mailowe), jest natrafienie na osoby, które w odpowiedzi na wiadomość przekażą nadawcy istotne dla niego informacje lub zainstalują na swoim komputerze złośliwe oprogramowanie umożliwiające przestępcy kontrolowanie komputera ofiary. Dlaczego spam phishingowy został zakwalifikowany jako przykład metody socjotechnicznej? Odpowiedź jest prosta: treść wiadomości jest napisana w taki sposób, by zmanipulować odbiorcę, uśpić jego czujność, przekonać go, że otrzymał wiadomość z zaufanego źródła (najczęściej z banku, w którym posiada swój rachunek bankowy), wpłynąć na niego w taki sposób, by podał poufne informacje umożliwiające uwierzytelnienie się w systemie bankowości elektronicznej lub zainstalował oprogramowanie pozwalające hakerowi na późniejsze monitorowanie jego czynności. Użytkownik, który uległ wpływowi odpowiednio spreparowanej informacji, nie zdaje sobie sprawy z faktu, iż sam spowodował wyciek krytycznych informacji, których nieuprawnione wykorzystanie może przysporzyć mu w najbliższym czasie kłopotów – nie tylko finansowych (wynikających z wykorzystania pozyskanych przez przestępcę informacji do dokonania operacji w systemie bankowym), ale i niewymiernych, związanych z utratą lub skopiowaniem danych znajdujących się w komputerze ofiary ataku.

Opisany powyżej proceder phishingu jest działaniem na oślep. Zawodowi przestępcy, wykorzystujący socjotechnikę do uzyskania oczekiwanych przez siebie korzyści, którym zlecono pozyskanie trudnej do zdobycia informacji, działają w sposób bardziej rozważny, są dobrze przygotowani do realizacji zadania. Aby zdobyć ważną, interesującą ich informację działają według opracowanego przez siebie planu. By dotrzeć do celu, nierzadko muszą pokonać kilka stopni – zinfiltrować środowisko, poznać procesy zachodzące w danej organizacji, jej strukturę, dane dotyczące poszczególnych pracowników firmy, nawet żargon branżowy. Przestępca robi to wszystko po to, by móc przekonać ofiarę, że jest jednym z pracowników firmy lub jej partnerów biznesowych, że można mu zaufać.

Od czasu do czasu środki masowego przekazu przestrzegają przed oszustami wyłudzającymi pieniądze od osób prywatnych, zazwyczaj starszych. Przestępca obiera za cel ataku osoby w podeszłym wieku, które są z reguły najbardziej podatne na oszustwo. Może na przykład posłużyć się starą książką telefoniczną (obecnie dane abonentów są lepiej chronione) i zadzwonić do osoby, której imię może kojarzyć się ze starszym pokoleniem (np. Antonina, Wiesława). W trakcie rozmowy telefonicznej może podszyć się pod bliskiego członka rodziny (np. wnuka) i przekonywać starszą osobę do udzielenia mu pożyczki, np. z racji kłopotów finansowych lub możliwości kupna samochodu za niezwykle atrakcyjną cenę. Jeśli przestępca wyczuje łatwowierność i uda mu się osiągnąć cel na tym etapie, może na przykład przyjść po „pożyczkę" jako kolega wnuka. W ten sposób oszuści są w stanie wyłudzić nawet kilkadziesiąt tysięcy złotych od niczego nie podejrzewających osób. Tego typu przestępstwa zdarzają się nadal, mimo iż przestrzegano przed nimi w mediach.

Istotną cechą ataków socjotechnicznych jest to, iż przestępca tylko w ostateczności posuwa się do bezpośredniego kontaktu „oko w oko" ze swoją ofiarą. Jest to dla niego zbyt niebezpieczne, gdyż mógłby zostać później rozpoznany lub jego wizerunek mógłby zostać utrwalony na nagraniach. Zazwyczaj przestępcy

wykorzystują do rozmów telefonicznych telefony komórkowe wyposażone w karty typu *pre-paid*, nie wymagające rejestracji danych użytkownika. Karty te oraz aparaty telefoniczne są po zakończeniu akcji niszczone, by uniemożliwić późniejsze namierzenie przestępcy. Przy dokonywaniu włamań do systemów informatycznych wykorzystywane są mechanizmy uniemożliwiające identyfikację miejsca, z którego dokonywany jest atak, oraz ustalenie, z jakiego komputera korzystał haker. Zdarza się również, że przestępca celowo wykorzystuje dostępną sieć (np. przełamując zabezpieczenia dostępnej domowej sieci wi-fi innego użytkownika mieszkającego w okolicy), by zmylić organy ścigania. Zazwyczaj socjotechnicy działają w taki sposób, że ofiara w ogóle nie zdaje sobie sprawy z faktu, że została zmanipulowana.

Jak bronić się przed oszustami, którzy wykorzystują metody socjotechniczne, by osiągnąć zamierzony cel? Po pierwsze zachować zdrowy rozsądek i nie dawać się ponieść emocjom – to gra na emocjach jest podstawową umiejętnością socjotechnika. Kolejną zasadą powinno być ostrożne spełnianie próśb osób, których nie jesteśmy w stanie rozpoznać po głosie – nawet jeśli dane identyfikacyjne podawane przez rozmówcę mogą wskazywać na to, że rozmówcą jest pracownik tej samej firmy. W takim przypadku, w celu weryfikacji rozmówcy, można zadzwonić do osoby, za którą rozmówca się podaje. Profesjonalista może jednak postarać się nawet o zastąpienie numeru pracownika firmy, za którego się podaje, swoim numerem telefonu.

W każdym przedsiębiorstwie – bez względu na liczbę zatrudnionych w nim osób – powinny obowiązywać przepisy dotyczące bezpieczeństwa informacji. W przepisach tych, oprócz sposobu klasyfikacji informacji (stopnia poufności, określenia roli „właściciela informacji" i procesu zarządzania informacją), powinny znaleźć się również zasady związane z bezpieczeństwem IT, dotyczące stosowania haseł systemowych o odpowiedniej złożoności (długość hasła, konieczność stosowania małych i wielkich liter, cyfr i znaków specjalnych), konieczności cyklicznej zmiany haseł, sposobu ich przechowywania, a także informacje dotyczące współpracy z kontrahentami. Powinien zostać wypracowany wzór umowy o zachowaniu poufności informacji. Taka umowa powinna też być częścią każdej umowy z firmą zewnętrzną, która będzie miała dostęp do pewnych informacji z racji współpracy. Równie ważnym elementem są szkolenia pracowników. Aby informacje firmowe były odpowiednio chronione, pracownicy muszą zdawać sobie sprawę z konieczności przestrzegania zasad bezpieczeństwa. Szkolenia z tego zakresu powinny być przede wszystkim merytorycznie wartościowe, ale pracownicy wyniosą z nich więcej, jeśli nie będą nudne. Odpowiednie przygotowanie programu edukacyjnego sprawi, iż kursanci zapamiętają więcej.

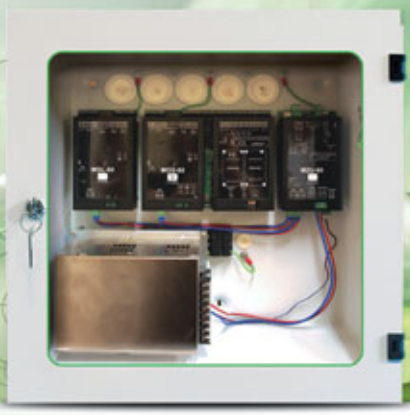
Zastanówmy się, jakie zasady bezpieczeństwa obowiązują w naszych firmach. Czy określają sposób klasyfikacji informacji oraz zasady współpracy z podmiotami zewnętrznymi w zakresie zachowania poufności informacji? Czy przepisy wewnętrzne przestrzegają na przykład przed otwieraniem e-maili z niewiadomego źródła i zapisywaniem dołączonych do nich plików? Czy wiadomo, jakich informacji nie powinniśmy udzielać nieznajomej osobie? Zastanów się, czy przypadkiem również z Tobą nikt nie przeprowadził rozmowy telefonicznej podobnej do tej, którą opisałem.

Krzysztof Białek

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

UCS 6000

UNIWERSALNA CENTRALA STERUJĄCA



WEJŚCIA	UCS 6000	WYJŚCIA
• **praca samodzielna** czujki przyciski oddymiania	 • ponad 20 wersji • niemal dowolna konfiguracja • dedykowany program konfiguracyjny • 5 lat gwarancji	• **sterowanie 24 V** klapy z siłownikami dwukierunkowymi 2 lub 3 przewodowymi klapy z siłownikami ze sprężyną sterowanie elektrotrzymaczami itp.
• **praca jako element adresowalny w systemie POLON 4000**		
czujnik deszczu i/lub wiatru przyciski przewietrzające		• **sterowanie 230 V~** wentylatory, kurtyny itp.

WSPÓŁPRACA Z CENTRALAMI SYGNALIZACJI POŻAROWEJ WSZYSTKICH PRODUCENTÓW

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

85-861 Bydgoszcz, ul. Glinki 155, www.polon-alfa.pl

Transmiter serwisowy

GSM TSG-1

Mariusz Radoszewski

Fot. 1. Transmiter TSG-1

Instalowane obecnie systemy bezpieczeństwa pożarowego w obiektach, w tym systemy sygnalizacji pożarowej oraz automatyki pożarowej, pełnią istotną rolę w ochronie mienia i życia ludzkiego. Często instalacje zabezpieczają bardzo ważne obiekty, w których niezawodność systemów ppoż. i ich niezakłócona praca są niezmiernie istotne. Aby zapewnić taki stan, służby odpowiedzialne za ich obsługę i serwis muszą niemal natychmiast dysponować informacjami o wszystkich uszkodzeniach i alarmach, np. generowanych przez centrale sygnalizacji pożarowej. Najszybszym i jednocześnie najprostszym sposobem powiadamiania o takich zdarzeniach jest wysłanie informacji przez sieć GSM

W czerwcu firma POLON-ALFA wprowadziła do swojej oferty transmiter serwisowy GSM TSG-1.

Transmiter jest urządzeniem umożliwiającym wysyłanie informacji (w formie wiadomości SMS) o zdarzeniach zarejestrowanych przez centrale sygnalizacji pożarowej firmy POLON-ALFA. Może również sygnalizować stan pracy różnych urządzeń posiadających wyjścia bezpotencjałowe. Wykorzystuje on sieć GSM i umożliwia pracę z kartami SIM różnych operatorów.

Komunikacja z adresowalnymi centralami sygnalizacji pożarowej odbywa się poprzez port szeregowy w standardzie RS232 z wykorzystaniem protokołu PMC-4000. Transmiter może współdziałać z następującymi centralami adresowalnymi produkcji POLON-ALFA: POLON 4100, POLON 4200, POLON 4500, POLON 4900.

Do wejść dwustanowych W1 i W2 można podłączyć dowolne urządzenie posiadające wyjście przekaźnikowe lub tranzystorowe „zwierające do masy". Mogą to być np. centrale konwencjonalne IGNIS 1000/2000 firmy POLON-ALFA, czujki autonomiczne ADR-20R lub centrale sygnalizacji włamaniowej.

Na obudowie transmitera znajduje się dioda LED sygnalizująca aktualny stan urządzenia. Opis poszczególnych stanów znajduje się w tabeli 1.

Stan diody	Stan transmitera
nie świeci	wyłączony
świeci ciągle	włączony, ale niezalogowany do sieci GSM
miga wolno	włączony i zalogowany do sieci GSM – czuwanie
miga szybko	włączony i zalogowany do sieci GSM w trakcie komunikacji z siecią

Tab. 1.

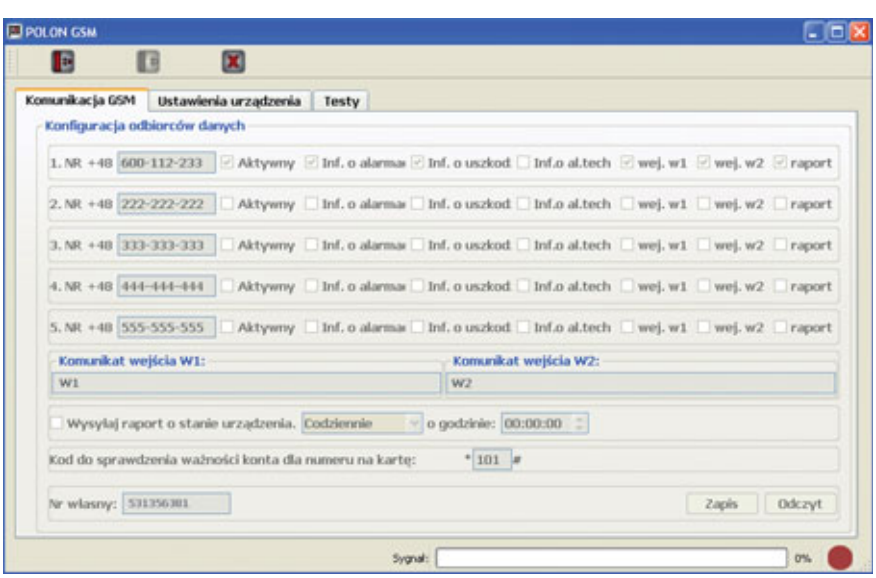
Konfiguracji transmitera TSG-1 dokonuje się za pomocą aplikacji POLON GSM dostępnej na stronie *http://www.polon-alfa.pl*. Komputer łączy się z transmiterem przez USB, przewodem z wtyczką mini USB dostarczonym razem z urządzeniem.

Urządzenie jest terminalem GSM firmy Sierra Wireless z oprogramowaniem przygotowanym przez firmę POLON-ALFA. Przed pierwszym uruchomieniem programu należy zainstalować sterowniki portu USB dla modemu AirLink FXT009 firmy Sierra Wireless. Program umożliwia wprowadzenie od jednego do pięciu numerów, na które będą wysyłane powiadomienia o zdarzeniach, jakie będzie rejestrował transmiter. Pierwszy numer jest traktowany jako nadrzędny i nie można go dezaktywować.

Gdy centrala sygnalizacji pożarowej zasygnalizuje pożar, uszkodzenie, uszkodzenie niemaskowalne lub alarm techniczny, transmiter wyśle informacje na numery telefonów, którym odpowiadają odpowiednie opcje. Transmiter TSG-1 jest urządzeniem wyłącznie serwisowym (nie służy do wysyłania informacji o alarmie pożarowym czy też uszkodzeniu), dlatego nie jest konieczne uzyskanie odpowiedniego certyfikatu dopuszczającego go do stosowania w ochronie przeciwpożarowej w Polsce.

mgr inż. Mariusz Radoszewski
POLON-ALFA

Fot. 2. Interfejs połączeniowy



Fot. 3. Okno wyboru numerów GSM

Zaawansowany System Kontroli Dostępu Wersja PREMIUM

KaDe

Kontrolery standardowe z portami RS lub IP
Czytniki w dowolnej technologii
Wizualizacja systemu na mapach
Integracja z systemem CCTV
Integracja z systemem RCP

Moduł przekaźnikowy
AL-1004

Kontroler standardowy
KS-1012-RS

Kontroler standardowy
KS-1024-IP

Czytnik
C-21

Czytnik
C-11

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Parametry systemu

4096 przejść kontrolowanych jednostronnie
20 000 użytkowników
50 000 zdarzeń w pamięci kontrolera

Oprogramowanie

KaDe wersja PREMIUM	Zaawansowana wersja programu nadzorczego dedykowana do współpracy z kontrolerami standardowymi w trybie sieciowym

Kontrolery standardowe i moduł przekaźnikowy

KS-1012-RS	Kontroler standardowy, 1 drzwi dwustronnie, 2 drzwi jednostronnie, 2 porty czytników, porty RS232 i RS485
KS-1024-RS	Kontroler standardowy, 2 drzwi dwustronnie, 4 drzwi jednostronnie, 4 porty czytników, port RS232 i RS485
KS-1012-IP	Kontroler standardowy, 1 drzwi dwustronnie, 2 drzwi jednostronnie, 2 porty czytników, port TCP
KS-1024-IP	Kontroler standardowy, 2 drzwi dwustronnie, 4 drzwi jednostronnie, 4 porty czytników, port TCP
AL-1004	Moduł przekaźnikowy przeznaczony do współpracy z kontrolerami standardowymi

Czytniki kart zbliżeniowych typu MIFARE (13,56 MHz)

C-11	Czytnik do instalacji wewnątrz i na zewnątrz pomieszczeń, format kodowania 34 bit Wiegand
C-21	Czytnik do instalacji wewnątrz i na zewnątrz pomieszczeń, format kodowania 26/34 bit Wiegand (przełączany), wyposażony w klawiaturę kodową (przełączany format 4/8 bit)
C-ADM-M	Czytnik kart administratora przeznaczony do wprowadzania dużej liczby kart MIFARE do bazy danych programu nadzorczego KaDe Premium. Istnieje możliwość wykorzystania urządzenia, np. do współpracy z dowolnym edytorem lub polami edytowalnymi w różnych aplikacjach.

System KaDe w wersji PREMIUM współpracuje z czytnikami w dowolnej technologii identyfikacji pod warunkiem, że posiadają interfejs Wieganda od 26 do 40 bit, czyli np. czytnikami kart UNIQUE, HID oraz innymi.

Kontrolowanie pracownika

Pracodawcy coraz częściej sprawdzają, jakie strony internetowe odwiedzają ich pracownicy, i kontrolują ich korespondencję. Czy takie działania są legalne?

Monika Brzozowska

W polskim prawie nie istnieją zapisy jednoznacznie regulujące kontrolowanie aktywności pracownika w sieci, jednak taka kontrola jest w interesie wielu pracodawców i uważają oni, że mają do niej prawo.

Monitorowanie aktywności pracownika w Internecie sprowadza się najczęściej do badania, jakie strony internetowe pracownik odwiedza i jakiej treści e-maile wysyła i otrzymuje. Tego typu działania należy oceniać, odwołując się do ustawy o ochronie danych osobowych, ale nie tylko. W Konstytucji są przecież wyłożone zasady ochrony wolności i praw człowieka i obywatela (art. 5 Konstytucji RP), ochrony godności człowieka (art. 30 Konstytucji RP), ochrony życia prywatnego, rodzinnego,

czci i dobrego imienia (art. 47 Konstytucji RP), wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji RP).

To oczywiste, że pracodawca, prowadząc działalność gospodarczą, dąży do maksymalizacji przychodów, w czym – bezpośrednio lub pośrednio – mają mu pomóc zatrudnieni pracownicy. Mamy jednak do czynienia ze swoistym konfliktem interesów. Z jednej strony bowiem istnieje prawo pracodawcy do ochrony własnych interesów gospodarczych, z drugiej zaś – prawo pracownika do wolności w sferze prywatnej, poszanowania jego dóbr osobistych i prawa jednostki (prawo do prywatności).

Pracodawca ma prawo kontrolować, czy pracownik sumiennie wywiązuje się ze swoich obowiązków pracowniczych, określonych treścią umowy o pracę oraz przepisami kodeksu pracy. Na mocy art. 22 kodeksu pracy pracownik, nawiązując stosunek prawny, zobowiązuje się do wykonywania pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem oraz w miejscu i czasie wyznaczonym przez pracodawcę. Warto również zwrócić uwagę na uregulowania wynikające z art. 100 kodeksu pracy, zgodnie z którymi do obowiązków pracownika należy sumienne i staranne wykonywanie pracy, stosowanie się do poleceń przełożonych, przestrzeganie czasu pracy, regulaminu pracy, porządku pracy, dbanie o dobro zakładu pracy i ochrona jego mienia. Pracodawca ma zatem prawo kontrolować, czy pracownik tych obowiązków przestrzega, a jedną z form kontroli może być cyfrowy monitoring pracowników. Ponadto celem monitorowania pracownika może być np. kontrola bezpieczeństwa przetwarzania danych lub przekazywania informacji mogących stanowić tajemnicę przedsiębiorstwa, a także zapobieganie popełnianiu przestępstw. Z drugiej strony należy jednak mieć na uwadze również treść art. 11 kodeksu pracy[1], zgodnie z którym pracodawca musi szanować godność i inne dobra osobiste pracownika.

Należy pamiętać, że wysyłanie prywatnej korespondencji, odwiedzanie stron internetowych (np. serwisów plotkarskich) czy przebywanie na portalach społecznościowych w czasie przeznaczonym na wykonywanie określonej pracy w zakładzie pracy może stanowić sprzeniewierzenie się pracownika jego obowiązkom, w szczególności obowiązkowi pracy w miejscu i czasie wskazanym przez pracodawcę (nieco bardziej złożony problem stanowią pracownicze konta pocztowe lub inne służbowe komunikatory, np. Gadu-Gadu, Skype). Działania podejmowane przez pracodawcę w celu kontroli aktywności pracowników mogą jednak kolidować z prawami pracownika do prywatności, zachowania treści korespondencji w tajemnicy i niewykorzystywania jego danych osobowych, jeśli ich wykorzystanie nie jest usprawiedliwione celami zatrudnienia. Tego typu działania pracodawcy nie muszą być nielegalne. Pracodawca powinien jednak poinformować pracowników o formie i zakresie prowadzonej kontroli, co w praktyce przyjmuje bardzo różne formy. Najczęściej odpowiednie zapisy znajdują się w regulaminie pracy, w samej umowie o pracę lub np. w stosownym aneksie.

Zgodnie z art. 49 Konstytucji RP każdy powinien mieć zapewnioną zarówno wolność komunikowania się, jak i możliwość utrzymania treści przekazu w tajemnicy. Ograniczenie jest możliwe w przypadkach określonych w ustawie i w określony w niej sposób. W tym przypadku można odnosić się do ustawy *Prawo telekomunikacyjne*, która w art. 159 ust. 2 określa sytuacje, w których tajemnica telekomunikacyjna może zostać ograniczona. Zgodnie z kodeksem cywilnym tajemnica korespondencji stanowi dobro osobiste każdego człowieka, przy czym należy odróżnić wolność komunikowania się od tajemnicy korespondencji z art. 23 kc. Zdaniem Sądu Najwyższego tajemnica korespondencji wynika z prawa „każdego człowieka do poszanowania jego życia prywatnego, (…) do zachowania w tajemnicy treści przekazu kierowanego do innych osób lub instytucji. Naruszenie tego dobra osobistego może nastąpić przede wszystkim przez bezprawne zapoznanie się z treścią korespondencji. Naruszenie tajemnicy korespondencji ma miejsce także wówczas, gdy (…) stworzono realne warunki (niebezpieczeństwo) umożliwiające, z dużym stopniem prawdopodobieństwa, zapoznanie się osób trzecich z jej treścią". Sąd Najwyższy zwrócił więc uwagę nie tylko na fakt zapoznania się z korespondencją (czyli np. z korespondencją pracownika), ale również stworzenia niebezpieczeństwa rozpowszechnienia takiej korespondencji.

Analizując kwestię monitorowania poczty e-mailowej, należy stwierdzić, że jeśli pracownik prowadzi jakąkolwiek służbową wymianę e-maili z kontrahentami i został poinformowany, że służbowe skrzynki służą jedynie do korespondencji służbowej, pracodawca ma prawo wglądu w taką korespondencję. Pracodawca nie ma natomiast prawa wglądu do korespondencji prywatnej. Jeśli jednak korespondencja prywatna pracownika jest zmieszana ze służbową, co może wynikać z konfiguracji konta pocztowego itp., pracodawca nie może – bez kontrowersji – kontrolować korespondencji służbowej pracownika.

Czy potrzebna jest zgoda pracownika na monitorowanie jego aktywności w miejscu pracy? Wydaje się, że możliwe są następujące rozwiązania:

1) Zgoda nie jest potrzebna, jeśli pracodawca dowiedzie, że przesłanką uzasadniającą monitorowanie pracowników jest jego prawnie usprawiedliwiony cel (zapobieganie stratom finansowym, zapobieganie naruszeniu tajemnicy przedsiębiorstwa, kontrolowanie bezpieczeństwa danych osobowych, zapobieganie popełnianiu przestępstw – np. ściąganiu treści nielegalnych lub instalowaniu nielegalnego oprogramowania) oraz że monitorowanie nie narusza praw i wolności osób, których dotyczy, a pracownicy są o nim poinformowani.
2) Zgoda jest potrzebna w każdym innym przypadku, przy czym nie wynika z innych oświadczeń woli i nie może być zgodą dorozumianą.

Pracodawca powinien uregulować kwestie dotyczące poczty e-mail w regulaminie pracy. Jeśli zezwala na użytkowanie służbowej skrzynki e-mailowej w celach prywatnych, powinny zostać opisane procedury dostępu pracodawcy do takiej skrzynki – takie, by dostęp ten nie naruszał ustawy o ochronie danych osobowych (np. stworzenie oddzielnego folderu na wiadomości prywatne na służbowym koncie pocztowym). Nie bez znaczenia jest również fakt, że właścicielem adresu e-mail, jako służbowego adresu danego pracownika, jest pracodawca. Na ten argument też warto zwrócić uwagę, ustalając dopuszczalność działań pracodawcy.

adwokat Monika Brzozowska
kierownik Departamentu Prawa Własności Intelektualnej i Danych Osobowych w kancelarii Pasieka, Derlikowski, Brzozowska i Partnerzy

1) Ustawa z dnia 16 lipca 2004 r. (DzU nr 171, poz. 1800 ze zm.).

Profesjonalna drukarka do nadruku na kartach PVC o większej długości

Rio PRO Xtended

Ultra ELECTRONICS | MAGiCARD

Magicard Rio Pro Xtended pozwala drukować na standardowych kartach ISO oraz na kartach o takiej samej szerokości, ale o większej długości. Daje to możliwość umieszczenia większej ilości informacji na powierzchni karty. Karta dzięki temu staje się bardziej czytelna. Obszar zadruku wynosi do 110×54 mm w pełnym kolorze, oraz 140×54 mm przy wydruku monochromatycznym. Drukarka obsługuje również karty predrukowane o długości do 140 mm. Wydruk zabezpieczany jest przeźroczystą warstwą Overlay, na której użytkownik ma możliwość wydruku spersonalizowanego znaku wodnego HoloKote lub HoloFlex.

Specyfikacja

- Typy wydruków: wydruk kolorowy i monochromatyczny na kartach standardowych oraz na kartach o większym formacie
- 3-letnia gwarancja Ultra CoverPlus obejmująca mechaniczne uszkodzenia głowicy oraz drukarkę zastępczą na czas naprawy
- Dostępne porty: USB i Ethernet w standardzie
- Sterowniki: Windows 2000 Professional (SP4), XP, Vista i 7 (32/64 bity), Windows Server 2003 R@SP2, Server 2008 (32/64 bity)
- Podajnik i odbiornik: Podajnik na 100 kart Xtended o wymiarach 86×140×54 mm, odbiornik na 70 kart Xtended o wymiarach 140×54 mm
- Masa: 4,95 kg
- Zasilanie: 100-240 V / 50-60 Hz
- Wymiary: 612×220×250 mm (wymiary obejmują podajnik i odbiornik)
- Prędkość nadruku: Wydruk karty w kolorze od krawędzi do krawędzi, 150 kart na godzinę
- Monochromatyczny nadruk karty 1000 kart na godzinę
- (Prędkość druku zależy od projektu graficznego karty)
- Temperatura pracy: od 10°C do 30°C

Powierzchnie wydruków

- Jednorazowy wydruk kolorowy 86×54 mm/86×50 mm
- Podwójny wydruk kolorowy 110×54 mm/110×50 mm
- Monochromatyczny 140×54 mm/140×50 mm

Zabezpieczenia kart

Możliwość wydruku znaku wodnego HoloKote. Do wyboru 4 standardowe znaki wodne, oraz znak wodny HoloFlex drukowany w dowolnym miejscu i dowolnym rozmiarze na powierzchni karty. Zarówno znak HoloKote i HoloFlex mogą być spersonalizowane w postaci dowolnego logo klienta.

Taśmy

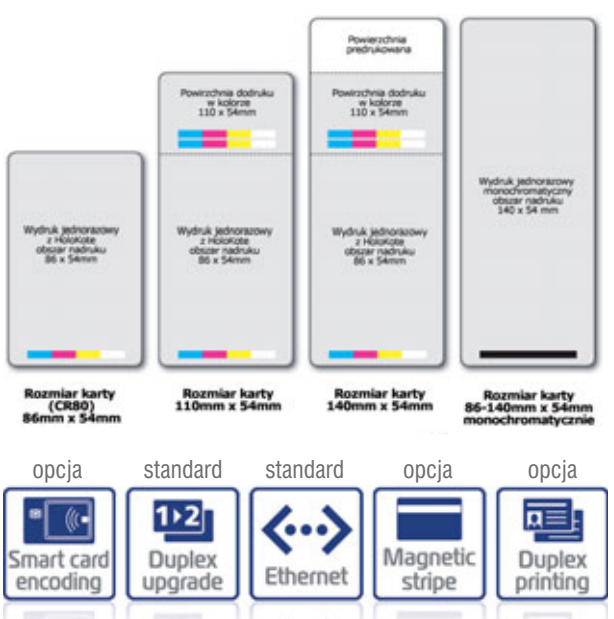
- YMCKO taśma kolorowana na 300 wydruków XXMA300YMCKO
- Taśmy monochromatyczne na 1000 wydruków: czarna, biała, niebieska, zielona, czerwona, srebrna, złota MA1000K

Zestaw czyszczący

- 1 szt. rolki czyszczącej dostarczana z każdą taśmą
- 10 szt. kart czyszczących
- 1 flamaster (3633-0053)
- 5 szt. wałków czyszczących plus wymienna oś wałka

Typy kart/grubości:

Wszystkie karty PVC ISO CR80/CR79, karty Xtended



Dystrybucja:

ACSS

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

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

Nowa drukarka do kart identyfikacyjnych

Ultra ELECTRONICS | MAGiCARD

Drukarka Enduro+ dostępna jest w wersji jedno- i dwustronnej. Wersja drukarki do nadruków jednostronnych może zostać w dowolnym momencie zaktualizowana przez użytkownika do wersji dwustronnej. W razie potrzeby użytkownik może również w prosty sposób rozbudować swoją drukarkę o port komunikacyjny Ethernet. Enduro+ wyposażona jest w podajnik kart wykorzystywany przy wydrukach seryjnych. Posiada również funkcję ręcznego podawania kart wygodną podczas wydruków pojedynczych. Drukarka umożliwia wydruk na zwykłych kartach PVC, kartach magnetycznych, zbliżeniowych, stykowych oraz kartach wielokrotnego zadruku i kartach samoprzylepnych. Obsługiwane są dwa formaty kart: CR-79 oraz CR-80.

Kluczowe cechy drukarki

- Jednostronny lub dwustronny nadruk od krawędzi do krawędzi
- Podajnik na 100 kart, odbiornik na 30 wydrukowanych kart
- Możliwość aktualizacji z drukarki jednostronnej do dwustronnej
- Możliwość ręcznego podawania kart
- Profil ICC (udoskonalane odwzorowanie kolorów)
- Kolorowy wyświetlacz LCD z przyciskami funkcyjnymi
- Możliwość drukowania na kartach do wielokrotnego zapisu
- Możliwość samodzielnej rozbudowy o port Ethernet

Zabezpieczenia

- HoloKote w standardzie 4 znaki wodne
- Wydruk na kartach HoloPatch (złoty kwadrat na powierzchni karty)
- Koder pasków magnetycznych (opcja)
- Koder kart stykowych, zbliżeniowych: MIFARE, DESFire, IClass (opcja)

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 35 s
- Monochromatyczny wydruk karty w 7 s
- TRW - Thermal Rewritable (wielokrotny zadruk termiczny)
- Interfejs do PC: USB rev. 1.1., USB 2.0 z opcją Ethernet
- Możliwość rozbudowy do wersji dwustronnej
- Menu wyświetlacza w języku polskim
- Sterowniki w języku polskim: Windows 2000 Proffesional (SP4), XP, Vista i 7 (32/64 bity), Windows Server 2003 R@SP2, Server 2008 (32/64 bity)
- Rozdzielczość wydruku: 300 dpi
- Podajnik na 100 kart
- Odbiornik na 30 kart
- Możliwość ręcznego podawania kart
- Zasilanie: 90-265 V / 47-63 Hz
- Wymiary / Masa: 453×233×206 mm/ 5,5 kg
- Temperatura pracy: od 10°C do 30°C
- Gwarancja: 2 lata

Taśmy

- Taśma kolorowana na 300 wydruków XXMA300YMCKO
- Taśmy monochromatyczne na 1000 wydruków: czarna, biała, niebieska, zielona, czerwona, srebrna, złota MA1000K

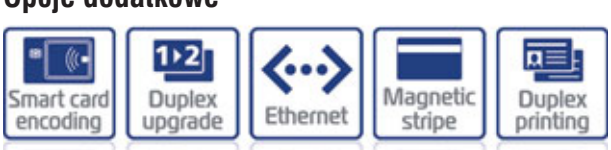
Karty

Drukuje na wszystkich standardowych kartach PCV ISOCR-80 (85,6×54) oraz CR-79 (84,1×52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch, kartach do wielokrotnego zadruku TRW.

Zestaw czyszczący

- 1 szt. rolki czyszczącej dostarczana z każdą taśmą
- 10 szt. kart czyszczących
- 1 flamaster (CK1)
- 5 szt. wałków czyszczących plus wymienna oś wałka

Opcje dodatkowe

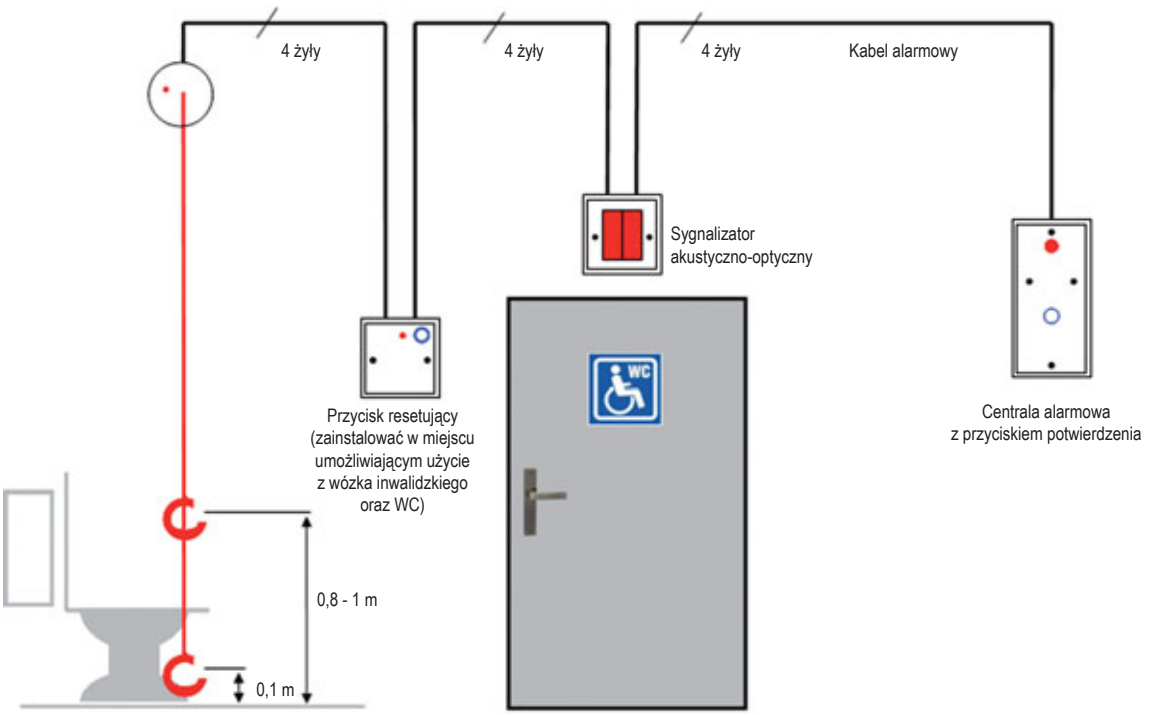


Dystrybucja: ACSS

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

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

Zestaw alarmowo-przywoławczy do toalet firmy Intercall



Przywoławczy zestaw do toalet jest prostym w instalacji i użytkowaniu oraz niezawodnym w działaniu systemem przywoławczym dla osób niepełnosprawnych. Przeznaczony do instalacji w toaletach i łazienkach umożliwia użytkownikom szybkie i proste wezwanie pomocy.

Zestaw zawiera wszystkie niezbędne urządzenia do zbudowania w pełni funkcjonalnego autonomicznego systemu przywoławczego. Dodatkowo do dyspozycji jest alarmowe wyjście przekaźnikowe NC umożliwiające integrację z innymi systemami. Centrala wyposażona jest w awaryjne zasilanie bateryjne zapewniające około 24 godziny pracy bez zasilania podstawowego. Istnieje możliwość rozbudowy zestawu o 2 dodatkowe przełączniki sufitowe.

Stan przywołania, aktywowany przy użyciu przełącznika sufitowego, sygnalizowany jest za pośrednictwem sygnalizatora akustyczno-optycznego przed wejściem do toalety oraz na panelu centralki alarmowej. Przywołanie może zostać skasowane za pomocą przycisku resetującego wewnątrz pomieszczenia. Zależnie od konfiguracji przywołania mogą być resetowane bądź potwierdzane za pomocą przycisku na centralce alarmowej. Jeżeli w czasie 120 sekund od potwierdzenia przywołania na centrali nie zostanie ono zresetowane za pomocą lokalnego przycisku resetującego wówczas centralka ponownie zasygnalizuje stan „alarm-przywołanie".

Cechy

- Wbudowany moduł zasilacza
- Wyjście przekaźnikowe
- Załączona bateria awaryjna
- Sygnalizacja dźwiękowa oraz świetlna
- Funkcja potwierdzenia przywołania
- Załączanie/Wyłączanie przycisku Reset
- Funkcja *self-test*
- Zdejmowane kostki połączeniowe
- 2 uchwyty typu G

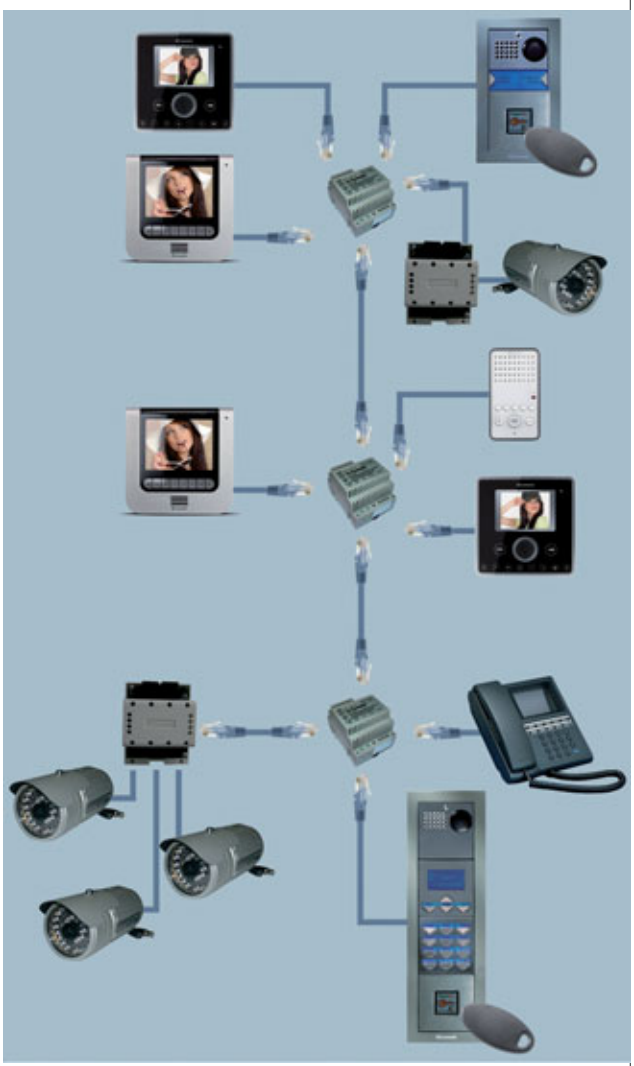
INTERCALL® SECURE SYSTEMS

Dystrybucja: alarmnet®

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

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

VIP – system wideodomofonowy IP
Połączenie nieograniczonych możliwości z prostotą instalacji



System wideodomofonowy Comelit VIP jest funkcjonalny, elastyczny i niezawodny. Prosty w instalacji i uruchomieniu.

Wykorzystanie technologii IP w każdym fragmencie systemu zapewnia niespotykane dotąd możliwości w tego typu aplikacjach.

W praktyce technologia ta daje projektantom i instalatorom wielką elastyczność i swobodę podczas projektowania, instalacji i późniejszej rozbudowy systemu.

Użytkownicy otrzymują już nie tylko narzędzie służące do rozmowy z gościem i otwarcia mu drzwi, lecz nowoczesny system komunikacji audiowizualnej o dużej funkcjonalności, a w przyszłości również możliwości integracji z innymi aplikacjami za pośrednictwem sieci LAN (np. TVIP, VIOP, PC, czy SmartPhone).

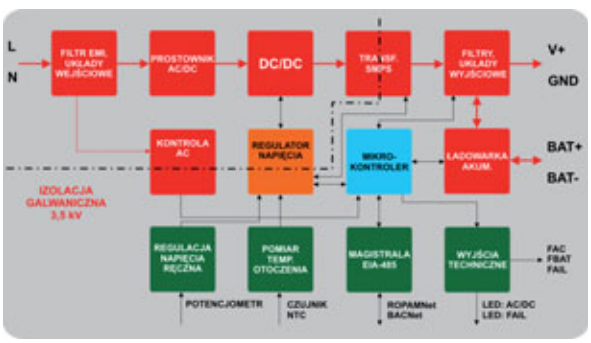
Wybrane funkcje i możliwości systemu VIP

- Technologia Plug & Play
- Brak limitu odległości pomiędzy urządzeniami
- Brak limitu liczby paneli głównych, lokalnych, central portierskich oraz monitorów wewnętrznych
- Wielka elastyczność. Brak narzuconej architektury połączeniowej. Każde urządzenie w systemie dołączane jest w ten sam sposób w dowolne miejsce na Switch'u
- Nieograniczona ilość równoległych rozmów. W systemie VIP całkowicie wyeliminowane zostało zjawisko zajętości
- Swobodne połączenia interkomowe. Możliwość komunikacji wewnętrznej pomiędzy wszystkimi użytkownikami systemu
- Proste programowanie. Podstawowe umiejętności obsługi komputera są wystarczające do uruchomienia systemu
- Możliwość zdalnej diagnostyki i obsługi systemu
- Wykorzystanie dedykowanej bądź istniejącej sieci LAN
- Monitory z pamięcią wideoklipów oraz możliwością nagrania komunikatu nieobecności
- Możliwość podglądu obrazu z kamer zewnętrznych oraz przekazania obrazu z kamer własnych do systemu CCTV
- Kontrola dostępu z czytnikami kart zbliżeniowych

Dystrybucja:

Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa
tel. 22 663 40 85, faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

PSR-ECO-5012-xx, PSR-ECO-5024-xx
Inteligentne, buforowe i nadzorowane zasilacze DC do systemów alarmowych oraz systemów automatyki



Firma Ropam Elektronik w wyniku analizy wymagań rynkowych oraz chcąc podążać za globalnymi trendami dotyczącymi poprawy efektywności wykorzystania energii wprowadza nowy standard w zasilaczach AC/DC. Unikalne parametry zasilaczy serii PSR-ECO można zgrupować w trzech blokach funkcyjnych.

1. Funkcje i parametry zasilacza AC/DC, blok przetwarzania energii

- Wysoka sprawność energetyczna, min. 88% w pełnym zakresie obciążeń roboczych
- Podwyższona separacja galwaniczna PRI/SEC: 3,5 kV (w innych zasilaczach ten parametr wynosi typowo: 1,5 kV)
- Moc wyjściowa 50 W w całym zakresie warunków II klasy środowiskowej
- Wersje 12 V_{DC} i 24 V_{DC}, zasilacz zapewnia ciągłość dostawy napięcia
- Regulacja napięcia wyjściowego, dotyczy zasilaczy DC
- Elektroniczne i autonomiczne zabezpieczenia: przeciążeniowe OCP, przeciwzwarciowe SCP, temperaturowe OHP, nadnapięciowe OVP, podnapięciowe UVP
- II klasa ochronności, bez obwodu PE
- Obudowa DIN 6M oraz dedykowane obudowy naścienne

2. Funkcje i parametry obwodu ładowania akumulatora

- Ładowanie akumulatora dwufazowe: stało-prądowe i stało-napięciowe
- Automatyczna kompensacja napięcia ładowania, +/- 3,3 [mV/°C/ogniwo] względem temperatury projektowej 25 °C
- Elektroniczne zabezpieczenia z automatycznym przywracaniem zasilania: OCP, SCP, UVP i odwrotną polaryzacją (RPP)
- Dynamiczny test i diagnostyka akumulatora
- Funkcja ochrony przed przeładowaniem uszkodzonego akumulatora: zaawansowany algorytm pomiaru wprowadzonego ładunku, jeżeli dostarczony zostanie wymagany ładunek, a zasilacz nie przejdzie w tryb ładowania stało-napięciowego to zasilacz wyłączy ładowanie, powiadomi o awarii jednak pomimo to pozostawi akumulator jako źródło zasilania awaryjnego
- Obsługa akumulatorów 12 V ołowiowo-kwasowych (SLA lub AGM)

3. Status pracy zasilacza (nadzór) i komunikacja systemowa

- Konstrukcja i funkcje zgodne z PN-EN 50131-6, stopień 2 lub 3, zasilacz typ A
- Mikroprocesorowa diagnostyka i kontrola pracy zasilacza
- Pomiar podstawowych parametrów zasilacza: I, U, temp.
- Wyjścia techniczne: stan AC, stan akumulatora oraz pozostałe awarie
- Magistrala EIA-485, protokoły komunikacji: ROPAMNet i BACNet (MS/TP, BACNet dostępny IVQ 2012)
- Nadzór i komunikacja z systemami NEO, VisumGSM (ROPAMNet) oraz BMS (BACNet)
- Optyczna sygnalizacja stanu pracy zasilacza
- Lokalna lub zdalna konfiguracja opcji zasilacza

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

VN-H157WPU
zewnętrzna kamera z serii Super LoLux HD

Kamera	
Przetwornik	1/3" SuperLoLux CMOS 1080P 2.2M
Liczba efektywnych pikseli	2,120,000 (1,944 H × 1,092 V)
Czułość	0.3 lx (przy IRE 50%, F1.2, AGC HIGH) 0.15 lx (przy IRE 25%, F1.2, AGC HIGH)
Tryb czarno-biały	< 0.05 lx (przy IRE 50%, F1.2,AGC HIGH) >
Sterowanie przysłoną	DC iris
Balans bieli	ATW/AWC
Funkcja rozszerzonej dynamiki	C.L.V.I. oraz Anti fog
Kompensacja światła tylnego	tak (4 opcje)
Obiektyw	
Typ mocowania	zintegrowany fabrycznie
Zakres zmian ogniskowej	3.0 mm to 9.0 mm, 3.0x vari-focal
Kąty widzenia	< 103° (H)×56° (V) ~ 35° (H)×20° (V) >
Maksymalna jasność/przysłona	F1,2
Zakres regulacji ustawienia obudowy kamery	horyzontalnie: +- 50°, wertykalnie: 90°, obrót: ± 110°
Inne	
Nagrywanie obrazów na kartę SD	tak
Wejście/wyjście alarmowe	2 x wejścia, 2 x wyjścia
Wyjście analogowe	Composite video signal: 1.0 V (p-p), PAL/ NTSC (RCA)
Fonia	wejście, wyjście
Zasilanie	24 V_{AC} (50 Hz/60 Hz)/48 V_{DC} (PoE)
Zużycie energii	0.5 A (24 V_{AC})/135 mA (PoE)
Temparatura pracy	-10 °C ~ 50 °C (bez grzałki)
Stopień szczelności obudowy	IP 66
Wymiary	140 mm × 167 mm × 257 mm (długość)
Masa	1,5 kg
Sieć	
Interfejs sieciowy	RJ-45: 10 BASE-T/100 BASE-TX
Protokoły sieciowe	TCP/IP, UDP/IP, FTP, ICMP, ARP, DHCP, SNTP, HTTP, DSCP, SMTP, RTP, IGMP, IPv6, HTTPS, SNMP, Zgodność z ONVIF, PSIA
Rozdzielczość obrazu	Wszystkie kompresje: 320×240, 640×480, MJPEG/H.264: 1 280×720, 1 280×960, 1 920×1 080
Kompresja (kodek)	MJPEG, H.264 (High/Baseline), MPEG-4
Liczba klatek na sekundę	30 dla H.264 (1 920×1 080), 30 dla MPEG-4 (640×480), 15 dla MJPEG (1 920×1 080)
Kompresja dźwięku	μ-law 64 kbps mono AD/DA 16-bitów
Bufor wewnętrzny	16 MB
Zabezpieczenie dostępu	3 poziomowe hasło, filtrowanie IP
Detekcja ruchu	tak
Web serwer	tak
Rodzaj transmisji	Unicast/Multicast

Kamery Super LoLux HD, w tym prezentowany model VN-H157WPU, potwierdziły, że problem słabej czułości kamer megapikselowych został rozwiązany i użycie takich kamer może być zalecane w przypadkach, w których dotychczas z założenia kamery megapikselowe nie mogły być stosowane (bez dodatkowego oświetlenia).

Dzięki zastosowaniu nowatorskiego procesora DSP, prawidłowa reprodukcja barw jest możliwa już przy oświetleniu na poziomie 0,3 luksa, co niejednokrotnie umożliwi identyfikację obserwowanych osób. To nowatorskie opracowanie oferuje także kompresję o wyższej wydajności. Kompresja H.264 realizowana przez procesor DSP w kamerach High Profile Super LoLux w odróżnieniu od popularnych rozwiązań stosowanych w kamerach Main Profile i H.264 Baseline Profile, umożliwia dystrybucję obrazów o wysokiej rozdzielczości, przyczyniając się jednocześnie do oszczędnego wykorzystania pasma sieciowego. Kamery sieciowe produkcji JVC są uwzględniane przez wielu producentów otwartych platform, są to między innymi Alnet Systems, Milestone, See Tec, Siemens, Axxon i Nuuo. Oprogramowania otwartych platform w standardzie ONVIF gwarantują pełną interoperacyjność pod warunkiem zaimplementowania całego SDK (kodów źródłowych). Oprogramowanie Milestone Xprotect Enterprise stanowi standardowe wyposażenie rejestratorów JVC - VR-X1600U (obsługujących maksymalnie 16 kamer) i VR-X3200U (obsługujących maksymalnie 32 kamery). Należy podkreślić, że kamery sieciowe firmy JVC odznaczają się bardzo wysoką niezawodnością, ich średni czas bezawaryjnej pracy (MTBF) wynosi 90000 godzin (ponad 10 lat).

Dystrybucja: euroalarm

EUROALARM Sp. J.
Bydgoszcz, ul. Piękna 25
85-303 Bydgoszcz

tel. 52 325 40 10
e-mail: biuro@euroalarm.com.pl
www.euroalarm.com.pl

PR102DR

Prosty i ekonomiczny kontroler dostępu serii zaawansowanej

Kontroler PR102DR jest nowym, ekonomicznym elementem systemu kontroli dostępu firmy ROGER. Urządzenie to zawiera wszystkie najistotniejsze funkcje i opcje dostępne w serii kontrolerów zaawansowanych. PR102DR może być stosowany samodzielnie lub w ramach systemu kontroli dostępu RACS 4 obejmującego różne kontrolery pojedynczego przejścia.

Charakterystyka

- Uproszczona konfiguracja
- Atrakcyjna cena
- Kontrola jedno lub dwustronna pojedynczego przejścia poprzez dołączenie czytników serii PRT (Roger)
- Obsługa do 4000 użytkowników
- Bufor pamięci na 32 000 zdarzeń
- Zasilanie z 12 V_{DC}
- Przekaźnik 5 A/30 V
- Dwie programowalne linie wejściowe NO/NC
- Jedna programowalna linia wyjściowa
- Dostępność w wersji do montażu na szynie DIN 35 mm oraz w postaci modułu elektronicznego
- Możliwość ustawiania adresu urządzenia na zworkach
- Wbudowany zegar czasu rzeczywistego z podtrzymywaniem bateryjnym

Producent: roger®

Roger Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

PR411DR-SET & PR402DR-SET
Zestawy kontroli dostępu

Akumulator widoczny na zdjęciu nie wchodzi w skład zestawu

PR411DR-SET i **PR402DR-SET** są zestawami złożonymi z kontrolera dostępu PR411DR lub PR402DR oraz zasilacza sieciowego PS-10ACDR (18VA) osadzonych fabrycznie w obudowie metalowej mogącej pomieścić akumulator awaryjny 7 Ah/12 V. Obudowa metalowa jest wyposażona w łącznik ochrony antysabotażowej oraz posiada wizjer do podglądu wskaźników statusowych zainstalowanych w niej urządzeń. Zestaw jest dedykowany do realizacji kontroli dostępu pojedynczego przejścia z jedno- lub dwustronną identyfikacją. Uzupełnieniem zestawu mogą być czytniki serii PRT produkcji ROGER lub inne czytniki pracujące w jednym z popularnych standardów takich jak Wiegand.

Zalety stosowania zestawów w rozwiązaniach kontroli dostępu:

- Atrakcyjna cena zestawu
- Kompletność rozwiązania – zestaw zawiera wszystkie (oprócz terminali) elementy potrzebne do realizacji punktu kontroli dostępu
- Możliwość instalacji na suficie
- Bezpośredni podgląd stanu pracy kontrolera dostępu dzięki wbudowanemu w obudowę wizjerowi
- Estetyczna metalowa obudowa
- Łatwa i szybka instalacja dzięki wyposażeniu w akcesoria montażowe

Zawartość zestawu:

- Kontroler dostępu PR411DR lub PR402DR
- Karta Master
- Komplet zworek do programowania adresu kontrolera
- Zasilacz transformatorowy PS-10ACDR
- Obudowa metalowa z wizjerem, łącznikiem antysabotażowym i szyną DIN 35 mm
- Komplet wkrętów mocujących
- Opaski zaciskowe do zamocowania akumulatora
- Komplet przewodów do podłączenia akumulatora
- Instrukcje obsługi

Producent: roger®

Roger Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

Kamera do montażu ukrytego
MBL-21S

Kamera MBL-21S to mini kamera o wysokiej czułości i bardzo wysokiej rozdzielczości (600 TVL w trybie kolorowym), wyróżniająca się bardzo dobrym i wiernym odwzorowaniem kolorów. Kolory są żywe i naturalne, a obraz ostry i wyraźny. Kamera jest przeznaczona do montażu ukrytego. Cechą wyróżniającą jest zastosowanie procesora Monalisa.

Zalety

- Regulacja położenia modułu kamery w dwóch osiach: pion, poziom
- SBLC – ulepszona odmiana BLC, czyli kompensacji tylnego oświetlenia
- Mini-obudowa metalowa
- Obiektyw 3,8 mm typu *pin-hole*

Właściwości

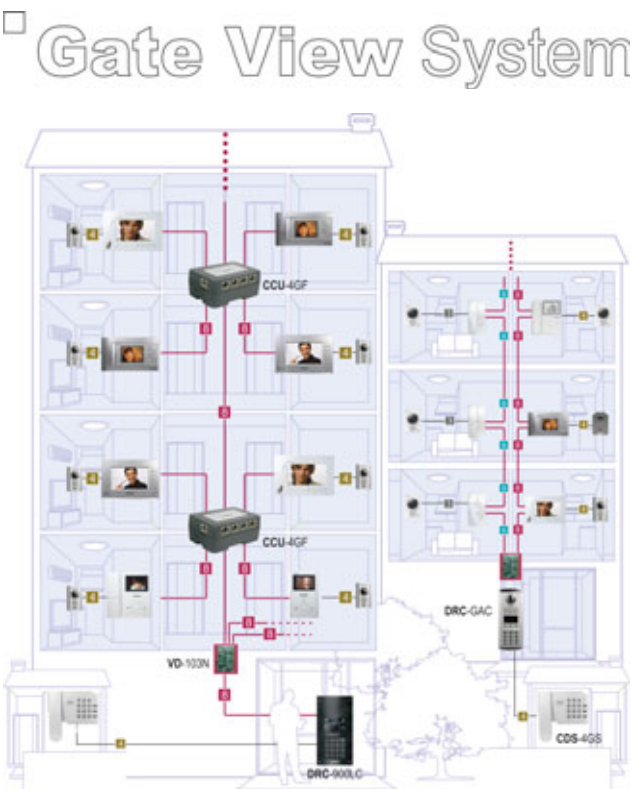
- Kamera kolorowa
- Przetwornik 1/3" Sony Super HAD II
- Bardzo wysoka rozdzielczość 600 TVL (kolor)
- Czułość 0,05 lx
- Obiektyw 3,8 mm typu pin-hole
- AGC, SBLC, AWB - automatyczne
- Zasilanie 12 V_{DC}
- Mini-obudowa metalowa

Standard sygnału wizyjnego	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD
Rozdzielczość efektywna	752(H)×582(V) 440K
Liczba linii telewizyjnych	600 TVL
Wyjście wizyjne	1,0V_{p-p}, 75 Ohm
Odstęp sygnał/szum	>50 dB
Obiektyw	f=3,8mm typu pin-hole
Tryb dzień/noc	brak
Czułość	0,05 lx
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja światła tylnego	SBLC, automatyczna
Elektroniczna migawka	1/50~1/120 000 s
Zasilanie	12 V_{DC}
Pobór prądu	maks. 250 mA/3 W
Wymiary	39 x 37 x 32,25 mm
Temperatura pracy/Wilgotność	-10°C~45°C / 30%~80% RH
Masa	210 g

Dystrybucja:
GDE Polska
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel./faks 12 256 50 35, 256 50 25
faks 12 270 56 96
e-mail: biuro@gde.pl

Wideodomofonowy system wieloabonentowy serii „Gate View”

COMMAX
SmartHome & Security



System wieloabonentowy serii „Gate View” przeznaczony jest zarówno do instalacji w blokach mieszkalnych jak i na osiedlach domów jednorodzinnych. Każdy lokator może posiadać kilka odbiorników wideodomofonych pozwalających na obsługę systemu z kilku miejsc.

Połączenia pomiędzy elementami systemu realizowane są przy użyciu kabla z parami skrętnymi UTP. Przy minimalnej konfiguracji do prawidłowego funkcjonowania niezbędne są jedynie panele zewnętrzne i odbiorniki (monitory). Dodatkowe elementy (wzmacniacze, rozdzielacze) pozwalają na rozbudowę systemu (kilka pionów, większa elastyczność).

Zastosowanie w systemie powszechnie dostępnego kabla sieciowego, wykorzystywanego w technice komputerowej jako medium transmisji sygnałów oraz separacja poszczególnych sygnałów na oddzielne pary przewodu pozwala osobom instalującym system w prosty sposób połączyć wszystkie jego elementy oraz szybko zlokalizować błędne połączenia czy uszkodzenia.

Dzięki połączeniu funkcjonalności monitorów analogowych z urządzeniami cyfrowymi system może być w prosty sposób rozbudowany przez dodanie indywidualnych paneli wejściowych lub dodatkowych kamer obserwacyjnych. Jeżeli na terenie obiektu znajduje się pomieszczenie ochrony, może ono być również wyposażone w stację portierską umożliwiającą kontakt ze wszystkimi użytkownikami oraz gośćmi. Lokatorzy korzystający z paneli bramowych mają możliwość otwarcia wejścia indywidualnymi kodami lub opcjonalnie kartą zbliżeniową. Różnorodność monitorów i paneli zewnętrznych pozwala dopasować wygląd sprzętu do wymogów architektonicznych projektowanych lub modernizowanych budynków.

Dystrybucja: &GDE POLSKA

GDE Polska
Włosań, ul. Świątnicka 88
32-031 Mogilany

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

AAT Holding sp. z o.o.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46
faks 22 546 05 01
e-mail: aat.warszawa@aat.pl
www.aat.pl

Oddziały:
ul. Koniczynowa 2A, 03-612 **Warszawa II**
tel./faks 22 743 10 11, 811 13 50
e-mail: aat.warszawa-praga@aat.pl

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

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

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

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

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

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

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

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

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

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

ABUS SECURITY CENTER
ABUS KEMAZ POLSKA Sp. z o.o.
ul. Wadowicka 8A
30-415 Kraków
tel. 12 640 15 60
faks 12 640 15 61
e-mail: tiglinski@abus-kemaz.pl
www.abus.pl

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

AGIS Fire & Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. 22 430 83 01
faks 22 430 83 02
e-mail: agisfs.pl@agisfs.com
www.agisfs.pl

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

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

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

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

ALPOL Sp. z o.o.
ul. Ścigały 10
40-208 Katowice
tel. 32 790 76 16
faks 32 790 76 60
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

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

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

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

ul. Paulinów 10, 67-200 **Głogów**
tel. 32 750 30 78
faks 32 750 30 69
e-mail: glogow@e-alpol.com.pl

ul. Sandomierska 105, 25-324 **Kielce**
tel. 32 720 39 82
faks 32 790 76 94
e-mail: kielce@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. Nowodworska 23, 59-200 **Legnica**
tel. 32 750 30 66
faks 32 750 30 67
e-mail: legnica@e-alpol.com.pl

ul. Grenadierów 13, 20-331 **Lublin**
tel. 32 790 76 50
faks 32 790 76 74
e-mail: lublin@e-alpol.com.pl

ul. Senatorska 31, 93-192 **Łódź**
tel. 32 790 76 25
faks 32 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. Długa 19, 63-400 **Ostrów Wlkp.**
tel. 32 750 30 25
faks 32 750 30 27
e-mail: ostrow@e-alpol.com.pl

ul. T. Kutrzeby 16G/112, 61-719 **Poznań**
tel. 32 790 76 37
faks 61 826 63 36
e-mail: poznan@e-alpol.com.pl

ul. Młodzianowska 75d, 26-600 **Radom**
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@e-alpol.com.pl

ul. POW 64, 98-200 **Sieradz**
tel. 32 750 30 55
faks 32 750 30 57
e-mail: sieradz@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. Polna 134/136, 87-100 **Toruń**
tel. 32 750 30 80
faks 32 750 30 73
e-mail: torun@e-alpol.com.pl

ul. Rzymowskiego 34, 02-697 **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. Spółdzielcza 3, 87-800 **Włocławek**
tel. 32 750 30 43
faks 32 750 30 45
e-mail: wloclawek@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

ul. Dekoracyjna 3, 65-722 **Zielona Góra**
tel. 32 750 30 70
faks 32 750 30 71
e-mail: zielona@e-alpol.com.pl

Zakład Produkcyjno-Usługowo-Handlowy
ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. 71 363 17 53, faks wew. 7
e-mail: anma@anma-pl.eu
www.anma-pl.eu

ASSA ABLOY POLAND Sp. z o.o.
ul. Jana Olbrachta 94
01-102 Warszawa
tel. 22 751 53 54
faks 22 751 53 56
e-mail: biuro@assaabloy.com.pl
www.assaabloy.com.pl

FIRMA ATLine Sp. J.
ul. Franciszkańska 125
91-845 Łódź
tel. 42 23 13 849÷851, 42 23 63 019
faks 42 655 20 99
e-mail: handel@atline.pl
www.atline.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 41 00
faks 22 715 41 05
e-mail: dominika.kolodziejska@pl.bosch.com
www.boschsecurity.pl

P.W.H. BRABORK-LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
tel. 22 619 29 49
faks 22 619 25 14
e-mail: brabork@braborklab.pl
www.braborklab.pl

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

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
Tulipan Hause
02-672 Warszawa
Infolinia 801 133 084
faks 22 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
86-050 Solec Kujawski
tel. 52 387 36 58, 387 54 66
faks wew. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

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

CMA MONITORING
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888
faks 22 546 0 619
e-mail: info@cma.com.pl
www.cma.com.pl

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

ul. Zatorska 36, 51-215 **Wrocław**
tel. 71 340 0 209
faks 71 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. 12 260 13 96
tel. kom. 665 380 677
faks 12 260 13 95

ul. Palacza 127, 60-279 **Poznań**
tel./faks 61 861 40 51
tel. kom. 601 203 664
e-mail: poznan@cma.com.pl

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

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

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

DYSKAM-EKOTRADE Sp. z o.o.
ul. Reymonta 22
30-059 Kraków
tel. 12 637 80 20
faks 12 637 80 20 wew. 23
e-mail: dyskam@dyskam.com.pl
www.dyskam.com.pl

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

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 812 05 05
faks 22 812 62 12
e-mail: sales@ebs.pl
www.ebs.pl

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

EL-MONT
ul. Wyzwolenia 15
44-200 Rybnik
tel. 32 423 07 28, 422 38 89
faks 32 423 07 29
e-mail: el-mont@el-mont.com
www.el-mont.com

PHU ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel. 22 398 96 53
faks 22 398 96 54
e-mail: elproma@elproma.pl
www.elproma.pl

EUREKA SOFT & HARDWARE
ul. Rynek 13
62-300 Września
tel. 61 437 90 15
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

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

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

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

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

GEO-KAT Sp. z o.o.
ul. Taneczna 7
02-829 Warszawa
tel. 22 877 08 80
faks 22 877 08 97
e-mail: info@geokat.com.pl
www.geokat.com.pl

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

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 98 44, 411 57 47
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

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

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. 32 324 89 00
faks 32 324 89 01
e-mail: firma@kabe.pl
www.kabe.pl

KATON Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa
tel. 22 869 43 92
faks 22 869 43 93
e-mail: biuro@katon.eu
www.katon.eu

KOLEKTOR
K. Mikiciuk i R. Rutkowski Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel./faks 58 553 67 59
e-mail: info@kolektor.pl
www.kolektor.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
faks wew. 28
e-mail: info@micronix.pl
www.micronix.pl

NOVATEL Sp. z o.o.
ul. Turystyczna 1
43-155 Bieruń
tel. 32 201 17 04
faks 32 201 15 11
e-mail: novatel@novatel.pl
www.novatel.pl

NUUXE – 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
www.nuuxe.com

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

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

Przedstawicielstwo:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks 32 202 55 82
e-mail: katowice@omc.com.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks 61 657 93 60
e-mail: poznan@omc.com.pl

ul. Różyckiego 1c, 51-608 **Wrocław**
tel./faks 71 347 91 91
e-mail: wroclaw@omc.com.pl

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 Sp. z o.o.
ul. Irysowa 11
02-660 Warszawa
tel. 22 831 15 35
faks 22 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

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

PROFICCTV Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. 61 842 29 62
faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl

PULSAR K. Bogusz Sp. J.
Siedlec 150
32-744 Łapczyca
tel. 14 610 19 40
faks 14 610 19 50
e-mail: norbert@pulsar.pl
www.pulsar.pl

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

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

RISCO GROUP POLAND Sp. z o.o.
ul. 17 Stycznia 56
02-146 Warszawa
tel. 22 500 28 40
faks 22 500 28 41
e-mail: sales-pl@riscogroup.com
www.riscogroup.com

ROPAM Elektronik s.c.
Os. Tysiąclecia 6A/1
32-400 Myślenice
tel. 12 341 04 07
faks 12 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.pl
www.ropam.eu

SAMSUNG TECHWIN EUROPE LIMITED
Biuro w Polsce
ul. Postępu 15c
02-676 Warszawa
tel. 22 20 50 777
faks 22 20 50 763
e-mail: STEsecurity@samsung.com
www.samsungsecurity.com

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
faks 17 857 79 99
e-mail: sawel@sawel.com.pl
www.sawel.com.pl

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

Oddziały:
CH Manhattan, III piętro
Al. Grunwaldzka 82, 80-244 **Gdańsk**
tel./faks 58 767 70 10
e-mail: gdansk@schrack-seconet.pl

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

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

P.T.H. SECURAL
ul. Gen. K. 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

SMA 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

Oddziały:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks 32 202 55 82
e-mail: katowice@sma.biz.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks 61 657 93 60
e-mail: poznan@sma.biz.pl

ul. Różyckiego 1C, 51-608 **Wrocław**
tel. 71 347 91 91
tel./faks 71 348 04 19
e-mail: sma@sma.wroclaw.pl

SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. Iłżecka 24
02-135 Warszawa
tel. 22 313 24 15, 511 84 64
faks 22 313 24 10
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.com

Oddziały:
ul. Arkońska 6 bud. A2
80-387 **Gdańsk**
tel. 58 782 00 01
faks 58 782 00 04

ul. Muchoborska 18
54-424 **Wrocław**
tel. 71 711 09 19
faks 71 711 09 20

ul. Krakowska 280
32-080 **Zabierzów k. Krakowa**
tel. 12 257 60 80
faks 12 257 60 81

SPS Electronics Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spselectronics.pl
www.spselectronics.pl

Biura Handlowe:
ul. Drożyny 6, 80-302 **Gdańsk**
tel. 58 624 83 04
faks 58 668 59 20
e-mail: gdansk@spselectronics.pl

ul. Kościuszki 227, 40-600 **Katowice**
tel. 32 255 64 27
faks 32 255 64 52
e-mail: katowice@spselectronics.pl

ul. Drewnowska 48, 91-002 **Łódź**
tel. 42 617 00 32
faks 42 659 85 23
e-mail: lodz@spselectronics.pl

ul. Polska 60, 60-595 **Poznań**
tel. 61 852 19 02
faks 61 825 09 03
e-mail: poznan@spselectronics.pl

ul. Grudziądzka 176, 87-100 **Toruń**
tel. 56 653 99 43
faks 56 653 90 81
e-mail: torun@spselectronics.pl

pl. Gen. Wróblewskiego 3a, 50-413 **Wrocław**
tel. 71 348 44 64
faks 71 348 36 35
e-mail: wroclaw@spselectronics.pl

STRATUS Sp. J.
ul. Nowy Świat 38
20-419 Lublin
tel./faks 81 743 87 72
e-mail: stratus@stratus.lublin.pl
www.stratus.lublin.pl

P.P.H.U. SUMA Sp. z o.o.
ul. Panewnicka 109
40-761 Katowice
tel. 32 258 05 97
faks 32 258 05 98
e-mail: biuro@suma.com.pl
www.suma.com.pl

Biuro Handlowe:
ul. Makuszyńskiego 22a/23, 31-752 **Kraków**
tel. 12 684 00 23
e-mail: krakow@suma.com.pl

TAP- Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: sprzedaz@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

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

UNICARD S.A.
ul. Łagiewnicka 54
30-417 Kraków
tel. 12 398 99 18
faks 12 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

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

VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. 61 623 23 05
faks 61 623 23 17
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

ZBAR PHU
Mariusz Popenda
ul. Krakowska 60
94-214 Łódź
tel. 42 611 12 98
faks 42 611 12 97
e-mail: zbar@zbar.com.pl
www.zbar.com.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ABUS	TAK	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS Fire & Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	TAK	–	–
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	–	TAK	–	TAK
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	TAK
FIRMA ATLine	–	TAK	TAK	TAK	–
BOSCH	TAK	–	–	–	–
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	–	TAK	–	–
CBC Poland	TAK	–	TAK	–	TAK
CMA	TAK	–	–	TAK	–
D-MAX	–	TAK	TAK	–	TAK
DG Elpro	–	TAK	TAK	TAK	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
Ela-compil	TAK	–	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
GEO-KAT	–	TAK	TAK	–	TAK
ICS POLSKA	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
Janex International	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
KATON	–	–	TAK	–	TAK
Kolektor	–	TAK	TAK	TAK	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
Novatel	TAK	TAK	TAK	TAK	TAK
Nuuxe – Radioton	–	TAK	TAK	TAK	TAK
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	TAK	TAK	TAK	TAK
RETT-POL	–	TAK	TAK	TAK	TAK
RISCO	TAK	–	–	–	–
ROPAM Elektronik	TAK	–	TAK	–	TAK
Samsung	TAK	–	TAK	–	–
Satel	TAK	–	–	–	–
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	TAK	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
SMA	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	TAK	–	TAK	–	–
SPS Electronics	–	TAK	TAK	–	TAK
STRATUS	–	TAK	TAK	–	–
SUMA	–	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Technokabel	TAK	–	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	TAK	TAK	–	TAK
ZBAR	–	TAK	TAK	TAK	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ABUS	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
AGIS Fire & Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	TAK	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
FIRMA ATLine	TAK	–	TAK	–	TAK	TAK	–	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	–	–	–
CMA	TAK	–	TAK	–	–	–	TAK	–	–
D-MAX	–	TAK	–	–	–	–	–	–	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Dyskam-Ekotrade	TAK	TAK	–	TAK	–	–	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	Transmitery IP/GSM/GPRS, systemy RFID, zabezpieczenia energetyka, bankowość, produkcja OEM/ODM								
Ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	TAK
FES	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	–	TAK	–
GEO-KAT	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
ICS POLSKA	TAK	TAK	TAK	TAK	TAK	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Janex International	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Novatel	–	–	–	–	–	TAK	–	–	TAK
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	TAK
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RETT-POL	TAK	TAK	TAK	TAK	–	–	–	–	–
RISCO	TAK	–	TAK	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SMA	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	–	–	TAK	–	–	–
SPS Electronics	TAK	TAK	TAK	TAK	–	–	TAK	–	–
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
SUMA	–	TAK	–	–	–	–	–	–	–
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
UNICARD	TAK	TAK	TAK	TAK	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	TAK	–	–	–
ZBAR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Paweł Karczmarzyk
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner
Andrzej Wójcik

Skład i łamanie
Tomasz Kaczmarczyk

Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. 22 546 0 951, 953
faks 22 546 0 959
www.zabezpieczenia.com.pl

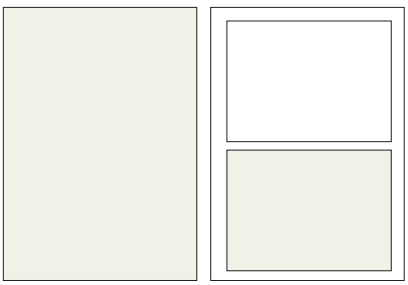
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4200 zł
cała strona, czarno-biała	2200 zł
1/2 strony, pełny kolor	2700 zł
1/2 strony, czarno-biała	1500 zł
1/3 strony, pełny kolor	1900 zł
1/3 strony, czarno-biała	1000 zł
1/4 strony, pełny kolor	1400 zł
1/4 strony, czarno-biała	800 zł
karta katalogowa, 1 strona	900 zł



cała strona (200 x 282 mm + 3mm spad)

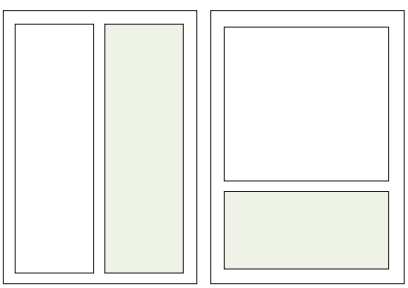
1/2 strony (170 x 125 mm)

Artykuł sponsorowany:

Cena za stronę artykułu sponsorowanego w czasopiśmie to 1500 zł (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



1/2 strony (83 x 260 mm)

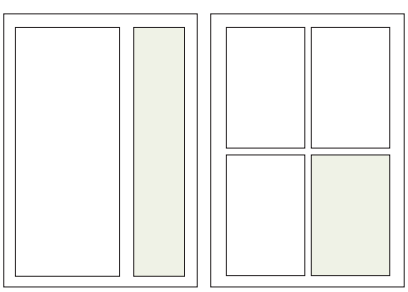
1/3 strony (170 x 80 mm)

Spis teleadresowy:

jednorazowy wpis 70 zł

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

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

Spis reklam

profesjonalne rozwiązania
do cyfrowej rejestracji obrazu

ponad 60 000 instalacji
pracujących na całym świecie

www.alnetsystems.com

ALNET SYSTEMS

sieciowe oprogramowanie do cyfrowej rejestracji obrazu — NS NETSTATION

hybrydowy system do cyfrowej rejestracji obrazu — NET HYBRID

hybrydowy system do cyfrowej rejestracji obrazu HD-SDI — NET HYBRID HD

profesjonalne oprogramowanie klienckie — CMS PROFESSIONAL

oprogramowanie klienckie dla urządzeń mobilnych — CMS MOBILE

blisko 1000 kamer zintegrowanych
z oprogramowaniem Alnet Systems

wybór należy do Ciebie!

ACTi · Arecont Vision · AXIS · BASLER · CRYPTOTELECOM · ETROVISION · GANZ
HIKVISION · iCANTEK · IQinVision · JVC · LILIN · Lumenera · PELCO · MESSOA
Panasonic · SANYO · SAMSUNG · SONY · StarBot · TOA · VIVOTEK · ZAVIO

Wykorzystaj nowe możliwości uwierzytelniania

Model Secure Identity Object firmy HID:

- **Zmienia każde urządzenie umożliwiające komunikację bliskiego zasięgu (NFC) w bezpieczne urządzenie uwierzytelniające**
- **Działa ze wszystkimi najpopularniejszymi kartami inteligentnymi**
- **Bezpieczne uaktualnienia ułatwiają migrację i zwiększają żywotność**

Przedstawiamy rozwiązanie iCLASS SE® z modelem danych Secure Identity Object (SIO).

Dowiedz się o SIO. hidglobal.com/sio lub zeskanuj kod przy użyciu czytnika QR

Bezpieczne i działające niezależnie od technologii nowe rozwiązanie iCLASS SE® pozwala zamienić telefony i inne urządzenia inteligentne w kartę identyfikacyjną.

HID®

Rozwiązanie iCLASS SE® umożliwia ochronę tożsamości przy użyciu wielowarstwowej, odpornej na złamanie technologii z bezpiecznym systemem zarządzania kluczem. Rozwiązanie to jest bardzo elastyczne — obsługuje technologie MIFARE®/DESFire®, EV1 oraz Indala, a także iCLASS®, umożliwiając przekształcenie każdego urządzenia obsługującego model danych SIO w bezpieczne urządzenie uwierzytelniające. Wybierz technologię i zaprogramuj nośnik uwierzytelnienia, aby już dziś stworzyć idealne rozwiązanie kontroli dostępu — następnie przeprogramuj czytnik, gdy zmienią się Twoje wymagania. Technologia iCLASS SE jest wszechstronna i elastyczna, została zaprojektowana z myślą o wysokiej wydajności. iCLASS SE to kontrola dostępu nowej generacji.

Więcej informacji można znaleźć w witrynie hidglobal.com/unleash-zab